Univerzita Karlova

Filozofická fakulta

Katedra pomocných věd historických a archivního studia

BAKALÁŘSKÁ PRÁCE

Barbora Dolejší

Šifrovaná korespondence v písemnostech válečné kanceláře Matyáše z Gallasu

Coded Correspondence among Documents of the War Office of Matthias von Gallas

Praha 2017

Vedoucí práce: Doc. PhDr. Ivana Ebelová, CSc.

Poděkování.

Na tomto místě bych v první řadě ráda poděkovala vedoucí práce paní doc. PhDr. Ivaně Ebelové, CSc. za cenné rady, trpělivost a čas věnovaný korekturám.

Mé díky patří také pracovníkům SOA v Litoměřicích – pobočky Děčín za vstřícný a ochotný přístup během mých badatelských návštěv.

Děkuji také Štěpánu Šimsovi za pomoc s úpravou práce.

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně, že jsem řádně citovala všechny použité prameny a literaturu a že práce nebyla využita v rámci jiného vysokoškolského studia či k získání jiného nebo stejného titulu.

V Praze dne 19. 8. 2017 Podpis

Abstrakt

Tato práce je příspěvkem k výzkumu raně novověkých šifer. Jejím cílem je rozbor šifrované korespondence, dochované mezi písemnostmi válečné kanceláře Matyáše Gallase. Jako celek jsou šifrované písemnosti nejprve zkoumány z hlediska jejich podílu vůči celkové agendě Gallasovy registratury. Na vybraném vzorku jsou následně představeny užívané typy šifer ve vojenském prostředí v době třicetileté války. Pozornost je věnována také otázce zachytávání dopisů nepřátelskou stranou. Nastíněn je rovněž obsah dopisů, přestože se uvedená práce zabývá šifrovanými písemnostmi primárně z hlediska paleografie. Zkoumaný vzorek šifrovaných dopisů je vybrán s ohledem na různé společenské sféry, z nichž pocházeli Gallasovi korespondenti, byť je patrná převaha osob z vojenského prostředí. Zároveň výběr pokrývá období prvního i druhého generalátu Matyáše Gallase, do kterých šifrovaná korespondence spadá. Součástí práce je také soupis všech šifrovaných písemností válečné kanceláře.

Klíčová slova: šifra, šifrovací klíč, nomenklátor, substituce, šifrovaná korespondence, Matyáš Gallas, třicetiletá válka

Abstract

This thesis is a contribution to the research of cryptography at the time of the early modern period. Its aim is to analyze coded correspondence found among other documents of the War Office of Matthias Gallas. First of all, the number of the coded documents is compared to the whole paperwork of Gallas's War Office to identify the ratio of encrypted writings. I also analyze sample letters to demonstrate kinds of ciphers that were used in military sphere during the Thirty Year's War. The sample of the coded letters is chosen in order to present correspondents of different social ranks even though the majority comes from commanders. I drew attention to a topic of letters intercepted by an enemy as well. I outline a content of a few chosen letters although the emphasis is mainly put on palaeography. Studied correspondence falls under the first two leadership periods of Matthias Gallas. A list of all encrypted documents is attached to this thesis as well.

Key words: cipher, encryption key, nomenclator, substitution, coded correspondence, Matthias Gallas, Thirty Years' War

Obsah

Seznam použitých zkratek

Úvod **7**

1 Charakteristika pramene a rozbor literatury **9**
1.1 Pramen 9
1.2 Literatura 11

2 Základní terminologie ke kryptologii **17**
2.1 Základní definice 17
2.2 Typy šifrovacích systémů 18

3 Matyáš Gallas na pozadí třicetileté války **20**

4 Analýza šifrované korespondence Gallasovy válečné kanceláře **25**
4.1 Podíl šifrované korespondence v rámci válečné kanceláře 25
4.2 Rozbor vybraných šifer 28
4.2.1 Šifra Matyáše Gallase s císařem Ferdinandem III. 28
4.2.2 Šifra Matyáše Gallase s Ferdinandem von Bayern 31
4.2.3 Šifra Matyáše Gallase a Ottavia Piccolominiho 33
4.2.4 Šifra Waltera Leslieho 36
4.2.5 Šifra Matyáše Gallase s markýzem di Grana a hrabětem Kurtzem 39
4.2.6 Zachycené šifrované dopisy na příkladu zpráv Lennarta Torstenssona 41

Závěr **45**

Seznam pramenů a literatury **47**

Seznam obrázků **53**

Seznam tabulek **53**

A Přílohy **54**
A.1 Soupis šifrovaných písemností 54
A.2 Příloha k šifrám pro korespondenci Gallase s císařem 86
A.3 Ukázky šifrovaných dopisů 89

Seznam použitých zkratek

AČ	Archivní časopis
HS	Historická sbírka
inv. č.	inventární číslo
kart.	karton
MIÖG	Mitteilungen des Instituts für Österreichische Geschichtsforschung
MÖStA	Mitteilungen des Österreichischen Staatsarchiv
sign.	signatura
SOA	Státní oblastní archiv

Úvod

Šifrování v historii patří k atraktivním tématům badatelů z řad odborné i laické veřejnosti. Mnoho publikací proto bylo věnováno jak dějinám utajování zpráv v minulosti, tak jednotlivým šifrovacím systémům a způsobům jejich prolomení.[1] Je proto s podivem, že v české odborné literatuře zůstává toto téma spíše na okraji badatelského zájmu.[2] Podrobněji se u nás tajným písmem v novověku zabýval Jaroslav Kašpar,[3] v současnosti se problematice šifrování věnuje Jakub Mírka, jehož článek *Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni* se stal podnětem ke vzniku této bakalářské práce.

V článku lze sledovat dva cíle. Kromě samotného představení šifrované korespondence napříč fondy šlechtických rodinných archivů, spadajících pod SOA v Plzni, si autor rovněž položil otázky obecného charakteru, tedy jaké typy šifer se objevují v období raného novověku a v jakém prostředí je můžeme hledat, jaké druhy zpráv se stávaly předmětem utajení a v neposlední řadě, jaké nároky byly kladeny na bezpečnost užívaných šifer a do jaké míry plnilo ono zabezpečení svou funkci v praxi. Na základě analýzy šifrovaných dokumentů v rámci jednoho státního oblastního archivu[4] je sice možné částečně formulovat odpovědi na výše uvedené otázky, avšak pro zobecnění získaných poznatků je nutné, jak autor v článku opakovaně zdůrazňuje, zevrubně prostudovat obdobný materiál i ve fondech ostatních státních oblastních archivů.[5]

V duchu tohoto závěru jsem se rozhodla podrobit hlubšímu studiu šifrovanou korespondenci válečné kanceláře Matyáše Gallase, která je součástí fondu Historická sbírka (rodinný archiv) Clam-Gallasů, Frýdlant, uloženého v SOA v Litoměřicích, pobočce Děčín – Podmokly. Původní záměr, tedy komplexní zpracování zkoumané části uvedeného fondu z hlediska klasické kryptografie[6] spolu s detailní

[1] O literatuře bude detailněji pojednáno v následující kapitole.

[2] Srov. KAŠPAR, Jaroslav. *Soubor statí o novověkém písmu.* Praha: Karolinum, 1993, s. 180; MÍRKA, Jakub. *Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni.* In: Západočeské archivy. Plzeň: Státní oblastní archiv v Plzni, 2012, s. 45.

[3] KAŠPAR, J. *Soubor statí*, s. 177-209; TÝŽ, *Příspěvek k řešení tajného písma ze 17. století.* In: Acta Universitatis Carolinae: Philosophica et Historica č. 5, 1963, s. 95-107.

[4] Pro účely srovnání využil autor i některé prameny uložené mimo SOA v Plzni, zejména písemnosti z fondů SOA v Litoměřicích – pobočka Děčín a SOA v Zámrsku. Nejednalo se ovšem o souhrnné zpracování šifrované korespondence v těchto fondech, nýbrž o výběr dokumentů, opřený převážně o edici ČECHOVÁ, Gabriela – JANÁČEK, Josef – KOČÍ, Josef – POLIŠENSKÝ, Josef (edd). *Documenta Bohemica belli tricennale illustrantia, Tomus I-VII.* Praha: Academia, 1971-1981. Srov. MÍRKA, J. *Raně novověká šifrovaná korespondence*, s. 44-45.

[5] Tamtéž, s. 44-45, 72.

[6] K dělení kryptografie, resp. kryptologie, na klasickou a moderní např. KLÍMA, Vlastimil. *Základy moderní kryptologie – Symetrická kryptografie I.* [online]. 2005, [cit. 4. 4. 2017]. Do-

historickou analýzou, se vzhledem k nalezenému množství pramenného materiálu ukázal jako neuskutečnitelný v rozsahu bakalářské práce. Stanovila jsem si proto za cíl, popsat soubor šifrovaných dokumentů a klíčů Gallasovy válečné kanceláře pomocí vhodně vybraných ukázek tak, aby byla pokryta celá doba existence kanceláře a současně co možná nejširší okruh korespondentů. Takto vytvořený nástin by měl kromě prvotního seznámení potencionálních čtenářů s tématem zároveň sloužit jako podklad pro pozdější navazující práci, v níž bych se ráda vrátila ke svému původnímu záměru.

Co se týče struktury předkládané práce, nejprve je pozornost věnována rozboru pramene a příslušné odborné literatury k historii šifrování. Jako nezbytná součást je dále uvedena základní terminologie, již užívám v souvislosti s popisem šifer a šifrovacích klíčů. V samostatné kapitole poté přináším stručný náčrt osobnosti císařského generála Matyáše Gallase s tím, že se zaměřuji právě na jeho úlohu ve třicetileté válce.[7] Stěžejní částí pak je čtvrtá kapitola, v níž je rozebrána šifrovaná korespondence Gallasovy válečné kanceláře. Rozbor je proveden na základě následujících otázek. Jaké je procentuální zastoupení šifrované korespondence v rámci celé válečné kanceláře? S kterými adresáty užíval Matyáš Gallas v korespondenci tajné písmo? Jaké typy šifer jednotliví adresáti užívali? Používali stále stejnou šifru, nebo ji v průběhu let měnili? Samozřejmě je nezbytné, ptát se i po obsahu zašifrovaných dopisů. Toho se u použitých ukázek také dotýkám, byť jsem si vědoma skutečnosti, že k detailnímu historickému výkladu pouhé vybrané příklady nestačí. Vedle uvedených otázek se zastavuji i u tématu zachycování šifrovaných dopisů nepřítelem a s tím souvisejícího problému bezpečnosti použité šifry. V závěru práce shrnuji zjištěné poznatky a pokouším se je, v rámci možností, alespoň částečně porovnat s výsledky článku Jakuba Mírky.

Přestože zde nemohu téma šifrované korespondence válečné kanceláře generál poručíka Gallase postihnout vyčerpávajícím způsobem tak, jak by zasluhovalo, přála bych si, aby tato práce aspoň do určité míry přispěla k současnému výzkumu raně novověkých šifer.

stupné z: `http://www.karlin.mff.cuni.cz/~tuma/nciphers/Symetricka_kryptografie_I.pdf`. Jedná se o text pro přednášku „Úvod do klasických a moderních metod šifrování“ na MFF UK. Podrobněji ke kryptologické terminologii viz níže.

[7] Toto pojetí je dáno jednak tématem bakalářské práce, v níž stojí Matyáš Gallas jako generál císařských vojsk, ale i faktem, že pro životní období Gallase mimo vojenskou kariéru existuje jen velice skrovná pramenná základna. Srov. REBITSCH, Robert. *Matyáš Gallas: (1588–1647). Císařský generál a Valdštějnův „dědic“*. Praha: Grada, 2013, s. 30.

1. Charakteristika pramene a rozbor literatury

1.1 Pramen

Předmětem studia předkládané práce je soubor šifrovaných písemností válečné kanceláře Matyáše Gallase. Hlubší rozbor tohoto souboru bude tedy v souladu s nastíněnými cíli proveden v samostatné hlavní kapitole. Považuji však za vhodné, zmínit se ve stručnosti o samotném archivním fondu, jehož je uvedená válečná kancelář součástí.

Gallasova válečná kancelář je dnes uložena ve fondu *Historická sbírka (rodinný archiv) Clam-Gallasů, Frýdlant* v SOA v Litoměřicích, pobočce Děčín – Podmokly. Přestože je celek označován jako fond,[8] vykazuje znaky, které ho řadí spíše k archivním sbírkám.[9] Jedná se o uměle vytvořený soubor archiválií, obsahující písemnosti více původců. Vedle rodinných dokumentů, týkajících se majitelů severočeských statků, a dokumentů majetkové povahy lze ve fondu nalézt i provenienčně různorodý materiál, shromážděný sbírkovou činností. Fond má celkový rozsah 132 běžných metrů[10] a je rozdělen do dvou částí.

První část byla rekonstruována na základě signatur, pocházejících z období pořádací činnosti gallasovských archivářů, z nichž patrně nejvýraznější stopu zanechal v tehdejším frýdlantském zámeckém archivu dr. Josef Bergl. Z praktického důvodu bylo nezbytné, zachovat během novodobého pořádání fondu ony původní signatury, pomocí nichž byly příslušné prameny častokrát uvedeny v literatuře.[11] Časové rozpětí této signované části je ohraničeno roky 1377, respektive 1272,[12] a 1943. Z kategorie rodinných písemností zde najdeme nejen prameny, vážící se k rodu Gallasů, Clamů a Clam-Gallasů, ale i dokumenty z pozůstalosti jejich předchůdců coby majitelů statků v severních Čechách, tedy Bibrštejnů a Redernů.

[8] Srov. SMÍŠKOVÁ, Helena. *Rodinný archiv (Historická sbírka) Clam-Gallas (1238)1529 - 1947. Inventář*, 1996, 306 s., ev. č. 1038.

[9] Jak napsala Helena Smíšková, která Historickou sbírku pořádala a inventarizovala: „Název Historická sbírka se traduje od dob prvních „státních“ archivářů, kteří tak výstižněji pojmenovali soubor pramenů různé provenience...“. Srov. SMÍŠKOVÁ, Helena. *Historická sbírka (rodinný archiv Clam-Gallasů)*. In: AČ. Praha: Sekce Archivní správy MV ČR, 1994, roč. 44, č. 3, s. 137.

[10] SMÍŠKOVÁ, H. *Inventář*, s. XXII. Naproti tomu evidence archivních fondů a sbírek na webových stránkách Ministerstva vnitra ČR v sekci Archivnictví a spisová služba uvádí celkový rozsah fondu (tzn. zpracované i nezpracované části) 118, 36 bm. [cit. 24. 04. 2017]. Dostupné z: `http://aplikace.mvcr.cz/archivni-fondy-cr`.

[11] SMÍŠKOVÁ, Helena. *Historická sbírka (rodinný archiv Clam-Gallasů) II. část*. In: AČ. Praha: Archivní správa MV ČR, 1998, roč. 48, č. 1, s. 23.

[12] K tomuto datu je v repertáři pánů z Bibrštejna uvedena listina, jejíž originál se však nedochoval. Srov. SMÍŠKOVÁ, H. *Historická sbírka*, s. 138.

V pěti kartonech jsou pak zachovány písemnosti z doby Albrechta z Valdštejna. Tato část fondu je ale významná i z hlediska množství rozmanitých pramenů k výzkumu hospodářských a sociálních poměrů v období 16.-19. století, k dějinám obcí a měst, patřících pod správu Gallasů, včetně záležitostí lokalit mimo české země. V neposlední řadě má dochovaný materiál badatelské využití i v otázkách vojenských, zvláště v souvislosti s třicetiletou válkou. Jedním z významných zdrojů, který pro studium tohoto konfliktu nabízí první část Historické sbírky, je právě v padesáti kartonech uložená válečná kancelář Matyáše Gallase. Obsahuje písemnosti z let 1627-1648 a pravděpodobně se tak jedná o celek zachovaný v úplnosti.[13]

Druhá část fondu žádné signatury neobsahovala, proto se při její inventarizaci postupovalo podle Zásad pro pořádání rodinných archivů a archivů velkostatků.[14] Přiřadit její písemnosti k signované první části na základě věcného hlediska nebylo možné, neboť ono hledisko nebylo během pořádání archivu gallasovskými archiváři pevně dodržováno. Dokumenty jedné záležitosti lze tedy najít na různých místech fondu. Časový rozsah druhé části spadá mezi roky (1238)[15] 1529-1947. Pramenný materiál je opět velmi pestrý. Obsahuje soubor listin (včetně císařských nebo valdštejnských), písemnosti dokumentující majetkové záležitosti, instrukce a vrchnostenská nařízení, militaria, dokumenty ve věcech církevních, torza pozůstalostí členů rodu Gallasů, Clamů, Clam-Gallasů, ale též pozůstalosti archivářů dr. Josefa Bergla a PhDr. Kurta Oberdorffera. Do této části fondu jsou zařazeny i sbírky rukopisů, tisků, otisků pečetí, novin a novinových výstřižků a další. Patří sem i skupina fotografií, pohlednic, rytin, map a plánů. Kromě uvedených archiválií se zde vyskytují i písemnosti, které provenienčně náleží do příslušných archivů velkostatků, z kterých je gallasovští archiváři vyňali a vložili do Historické sbírky.[16]

Protože je fond de facto sbírkou pramenného materiálu, který sice v mnoha případech nemá žádný vztah k původnímu rodinnému archivu Clam-Gallasů nebo k dokumentům jejich statků, avšak podává svědectví o jejich zájmech, byl ponechán během novodobého pořádání téměř v úplnosti jen s minimem skartačních zásahů.[17]

[13] Tamtéž, s. 138-140.

[14] SMÍŠKOVÁ, H. *Inventář*, s. V.

[15] Pod tímto datem je uveden kopiář listin kláštera Marienthal. Srov. SMÍŠKOVÁ, H. *Historická sbírka II. část*, str. 18.

[16] Tamtéž, str. 18-22.

[17] SMÍŠKOVÁ, H. *Inventář*, s. XV.

1.2 Literatura

O šifrování obecně, ať již ve smyslu šifrovacích systémů, respektive jednotlivých šifer, nebo z hlediska dějin kryptologie bylo pojednáno v mnoha publikacích odborných i populárně-naučných. Pro následující rozbor byly vybrány některé z prací, jež jsou relevantní pro historika či archiváře, který zkoumá tajné písmo z pohledu paleografie nebo ve snaze rozluštit zašifrovaný historický pramen[18] a jehož výzkum se orientuje na středoevropské prostředí.

Velmi dobrou průpravou v oblasti nejrůznějších způsobů šifrování je kryptologická příručka *Eduarda B. Fleissnera von Wostrowitz*,[19] rozdělena do tří částí. První z nich je uvozena všeobecným poučením o kryptografii, kde autor mimo jiné definuje základní pojmy, požadavky pro kvalitní tajné písmo a pravidla, užívaná u většiny tajných písem. Následně jsou představeny různé typy šifer. U každého typu jsou rozebrány jednotlivé varianty, u nichž je uveden názorný příklad a návod, jak probíhá dešifrování. V této části Fleissner vycházel ze staršího díla *Johanna Ludwiga Klübera*.[20] Celá druhá část se zabývá metodou utajení pomocí otočné mřížky. Ta byla známa a popsána již dříve, avšak Fleissner jí a jejím variantám věnoval mimořádnou pozornost. Proto bývá tento typ transpoziční šifry označován jako Fleissnerova mřížka.[21] Obsahem třetí části je pak luštění jazykově německých tajných sdělení bez znalosti klíče, a to po teoretické i praktické stránce. Příručku doplňují příklady šifrovacích klíčů pro ukázku některých šifer první části.

Podobně koncipována je i publikace *Ernsta Dröschera*.[22] Jedná se o přehledovou práci o metodách šifrování, které jsou rozděleny do dvou kategorií, a sice tajné písmo zjevné, u něhož je na první pohled zřejmé, že se jedná o šifru, a tajné písmo skryté. Ve druhé skupině jsou popsány takové způsoby utajení textu, který sice po zašifrování zůstává sám o sobě viditelný, avšak fakt, že se ve skutečnosti jedná o šifru, je znám pouze příjemci zprávy. Na rozdíl od Fleissnerovy příručky se tato kniha zaměřuje jen na podstatu jednotlivých šifer s nástinem jejich původu

[18] Zcela stranou tedy budou ponechány kryptologické publikace z oborů matematiky a informatiky, s nimiž zejména moderní kryptologie úzce souvisí.

[19] FLEISSNER VON WOSTROWITZ, Eduard B. *Handbuch der Kryptographie. Anleitung zum Chiffriren und Dechiffriren von Geheimschriften.* Wien: In Commission bei L. W. Seidel & Sohn, 1881.

[20] Tamtéž, s. 6.
KLÜBER, Johann Ludwig. *Kryptographik. Lehrbuch der Geheimschreibekunst (Chiffrir- und Dechiffrirkunst) in Staats- und Privatgeschäften.* Tübingen: J. G. Cotta'schen Buchhandlung, 1809. Kromě popisu metod šifrování a způsobů dešifrování (včetně speciálních návodů pro různé jazyky) podává Klüber i soupis literatury, týkající se šifrování.

[21] Srov. např. BAUER, Friedrich L. *Historische Notizen zur Informatik.* Berlin: Springer, 2009, s. 334; KLÍMA, Vlastimil. *Utajené komunikace – 4. díl: Od novověku do 20. století.* In: Chip: počítačový magazín. Praha: Vogel Publishing, 1994, roč. 4, č. 8, s. 120.

[22] DRÖSCHER, Ernst. *Die Methoden der Geheimschriften (Zifferschriften) unter Berücksichtigung ihrer geschichtlichen Entwicklung.* Leipzig: K. F. Koehler, 1921.

a až na výjimky neobsahuje názorné příklady či pasáže o dešifrování. Obsahuje ale shrnutí literatury s uvedením teoretických prací od pozdního středověku do Dröscherovy doby, na něž autor upozorňuje v souvislosti s absencí podrobného rozboru jednotlivých šifrovacích metod a postupů při jejich dešifrování.[23]

Převážně kryptoanalyticky je zaměřen článek *Wilhelma Gerlicha*,[24] jenž na dvou příkladech demonstruje možnosti rozluštění textů utajených pomocí substituční šifry. Použité zásady jsou pak obecně shrnuty v závěru článku. Za povšimnutí dále stojí fakt, že Gerlich považuje kryptografii za pomocnou vědu historickou.[25]

Historický vývoj a užívání tajného písma se snažil objasnit *Friedrich Wagner*.[26] V souhrnné studii, rozdělené do tří částí, podrobně rozebírá jednotlivá díla věnovaná kryptologii od doby Johanna Trithemia[27] až po práce svých současníků. Věnuje se spisům německých, italských, francouzských a anglických autorů. V souvislosti s dějinami šifrování nelze opomenout rozsáhlou a často citovanou publikaci *Davida Kahna*, popisující historii užívání tajného písma od starověkého Egypta až do 20. století.[28]

Užíváním tajného písma v období středověku se zabýval *Bernhard Bischoff* v článku přehledového charakteru.[29] Ten je rozdělen do několika částí podle typu šifry, jejíž varianty a použití uvádí na příkladech konkrétních středověkých rukopisů několika evropských států. V případě popisovaných šifer se jedná o nejjednodušší substituční i transpoziční metody utajení.

Ohledně šifrování ve středověku je třeba alespoň krátce připomenout dílo *Aloyse Meistera*, týkající se užívání tajného písma v prostředí papežské kurie v době od jejího počátku do přelomu 16. a 17. století.[30] V první části je po-

[23] Tamtéž, Vorwort.

[24] GERLICH, Wilhelm. *Die Entzifferung von historischen Geheimschriften.* In: MÖStA Bd. 1, 1948, s. 445-469.

[25] Tamtéž, s. 445.
V tomto ohledu není jediný. Na kryptografii jako na pomocnou vědu historickou nahlíží i jiní autoři. Např. FURLARI, Silvio. *La stenografia e la crittografia – scienze ausiliarie della storia.* In: Römische Historische Mitteilungen 31, 1989, s. 578-589. Srov. HLAVÁČEK, Ivan - KAŠPAR, Jaroslav - NOVÝ, Rostislav. *Vademecum pomocných věd historických.* 5. upravené a doplněné vydání, Jinočany: H & H, 2015, s. 109.

[26] WAGNER, Friedrich. *Studien zu einer Lehre von der Geheimschrift (Chiffernkunde).* In: Archivalische Zeitschrift Bd. 11 (1886), s. 156-189; Bd. 12 (1887), s. 1-29; Bd. 13 (1888), s. 8-44.

[27] Německý učenec a humanista Johannes von Heidenberg, zvaný též Trithemius (podle rodiště Trittenheim nad Moselou), žil mezi lety 1462-1516. Působil jako opat kláštera ve Sponheimu, později pak ve Würzburgu v klášteře sv. Jakuba. Pro kryptologii je významný zejména jeho šestidílný spis *Polygraphiae*. Po Trithemiovi je rovněž pojmenován typ polyalfabetické substituční šifry. Srov. WAGNER, F. *Studien*, Bd. 11, s. 160.; VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma.* Praha: Albatros, 2006, s. 59-61, 219.

[28] KAHN, David. *The Codebreakers: the story of secret writting.* New York: Scribner, 1996.

[29] BISCHOFF, Bernhard. *Übersicht über die nichtdiplomatischen Geheimschriften des Mittleralters.* In: MIÖG 62, 1954, s. 1-27.

[30] MEISTER, Aloys. *Die Geheimschrift im Dienste der päpstlichen Kurie: von ihren Anfängen bis zum Ende des XVI. Jahrhunderts.* Paderborn: Schöningh Verlag, 1906.

dán teoretický výklad, v části druhé jsou otištěny odpovídající prameny, a to jak traktáty o šifrování a dešifrování, tak sbírka klíčů. Meister se šifrováním zabýval i v souvislosti s italskými písemnostmi diplomatické sféry v 15. století,[31] v nichž spatřuje počátky moderní kryptologie. Podle Meistera lze totiž v Itálii v uvedené době hledat kořeny moderní diplomacie, a to díky rozmachu vysílání vyslanců k cizím dvorům. S tím pak v konečném důsledku souvisí právě rozvoj tajného písma, neboť *„je notwendiger die Gesandten wurden, desto notwendiger auch die Kryptographie.“*[32]

Vedle teoretických či přehledových pojednání o šifrování existují i práce s úzce vymezeným předmětem zkoumání. K takovým lze zařadit knihu *Ericha Hüttenhaina* o užívaných šifrách v knížecím biskupství Münster za doby biskupa Christopha Bernharda von Galen.[33] Věnuje se v ní souboru 33 šifrovacích klíčů (z nichž 30 bylo dochovaných a tři rekonstruované z příslušných dopisů) určených pro tajnou korespondenci Christopha Bernharda s jeho vyslanci na zahraničních dvorech.[34] Historií a organizací tajné šifrovací kanceláře ve Vídni se zabýval *Franz Stix*.[35]

S přihlédnutím k tématu a postupu při zpracování této bakalářské práce připomeňme tři články autorky *Hildegard Ernst*. Ve dvou z nich se zabývá výměnou šifrovaných dopisů mezi říšskou kanceláří, císařskými vyslanci v Madridu a bruselským dvorem v letech 1635-1642,[36] které nalezla mezi ostatními prameny pro svou disertační práci, věnovanou politickým a finančním vztahům Vídně a Madridu mezi lety 1632-1637.[37] V uvedených článcích analyzuje celkem 6 šifer, popisuje několik způsobů, jakými se jí podařilo získat příslušné šifrovací klíče - rekonstrukci na základě dešifrovaných pasáží textu, frekvenční analýzu nebo rozluštění díky chybě či nedbalosti písaře. V této souvislosti si všímá i odolnosti užívaných šifer vůči náhodnému rozluštění a preventivních opatření, která tomu měla zabránit. Stranou autorčina zájmu nezůstává ani obsah dopisů a způsob doručování. Třetí článek Hildegardy Ernst, a sice o tajných písmech Habsburků během třicetileté války,[38] z větší části koresponduje s výše uvedenými články. Stojí však za samo-

[31] Týž. *Die Anfänge der modernen diplomatischen Geheimschrift*. Paderborn: Schöningh Verlag, 1902.

[32] Tamtéž, s. 14.

[33] HÜTTENHAIN, Erich. *Die Geheimschriften des Fürstbistums Münster unter Christoph Bernhard von Galen 1650-1678*. Münster: Aschendorff, 1974.

[34] Tamtéž, s. 7.

[35] STIX, Franz. *Zur Geschichte und Organisation der Wiener Geheimen Ziffernkanzlei. (Von ihren Anfängen bis zum Jahre 1848.)*. In: MIÖG Bd. 51, 1937. s. 131-160.

[36] ERNST, Hildegard. *Geheimschriften im diplomatischen Briefwechsel zwischen Wien, Madrid und Brüssel 1635-1642*. In: MÖStA Bd. 42, 1992, s. 102-127; TÁŽ, *Geheimschriften im diplomatischen Briefwechsel zwischen Wien, Madrid und Brüssel 1635-1642 (Teil II)*. In: MÖStA Bd. 45, 1997, s. 207-232.

[37] TÁŽ, *Geheimschriften*, s. 102.

[38] TÁŽ, *Geheimschriften der Habsburger im Dreißigjährigen Krieg*. In: Siglo de Oro – Decadencia. Spaniens Kultur und Politik in der ersten Hälfte des 17. Jahrhunderts, hrsg. von Heinz Duchhardt/Christoph Strosetzki. Köln, Weimar, Wien: Böhlau Verlag, 1996, s. 95-108.

statnou zmínku, protože se vedle problematiky šifrování v rámci diplomatických kontaktů španělského a císařského dvora v krátkosti zabývá i šifrou, kterou užíval v letech 1641-1642 císař Ferdinand III. ve vlastnoruční korespondenci se svým bratrem, arcivévodou Leopoldem Vilémem, toho času vrchním velitelem císařských vojsk.[39] Šifra je zajímavá z několika důvodů. Předně se zdá, že neodpovídá vzoru běžných šifrovacích systémů, což autorku vede k domněnce, že si zřejmě detailně propracovanou šifru vymyslel císař, jeho bratr nebo oba dva speciálně pro svoji vzájemnou korespondenci. Některé indicie navíc nasvědčují tomu, že i vlastní zašifrování prováděl císař sám a dokonce pravděpodobně utajoval existenci šifry před svými sekretáři. Nedochoval se klíč ani přepisy šifrovaných pasáží[40] a pokusy o prolomení šifry dosud nebyly úspěšné.[41] Z nešifrovaných částí dopisů je zřejmé, že vedle osobních záležitostí řešili převážně věci politické a vojenské.

V únoru roku 2013 se v německém městě Gotha konala mezinárodní konference na téma utajování zpráv diplomatické korespondence na evropských dvorech v raném novověku, na které zazněly příspěvky k šifrování jak obecného, tak specifického charakteru.[42] Z konference později vznikl sborník přednesených referátů.[43]

Odborná literatura o šifrování z pera českých autorů zatím není příliš početná. Roku 1858 podal krátkou zprávu jičínský gymnaziální profesor *Antonín Vánkomil Maloch*[44] o tom, že se mu podařilo rozluštit český zašifrovaný lístek, který nalezl Václav Hanka mezi částečně šifrovanou korespondencí ke vpádu pasovským do Čech roku 1611.[45] S povzdechem nad banalitou utajeného sdělení zveřejnil jeho

[39] Roku 1639 převzal Leopold Vilém vrchní velení po Matyáši Gallasovi. Srov. HÜTTL, Ludwig. *Leopold Wilhelm.* In: Neue Deutsche Biographie 14, 1985, s. 296-298 [online]. [cit. 31. 5. 2017]. Dostupné z: `https://www.deutsche-biographie.de/gnd118727664.html#ndbcontent`.

[40] Ernst, H. *Geheimschriften der Habsburger*, s. 101-102.

[41] V případě prolomení šifry plánovala Hildegard Ernst její zveřejnění ve 47. svazku MÖStA v roce 1999. Srov. Ernst, H. *Geheimschriften Teil II*, s. 207. V onom vydání k tomu ale nedošlo. Pomocí počítače se pokusil o rozluštění německý informatik *Albrecht Beutelspacher* se skupinou studentů. Srov. Ernst, *H. Geheimschriften der Habsburger*, s. 102. Šifrou se zabýval i informatik *Klaus Schmeh*, expert na historickou kryptoanalýzu, který odhalil část znaků. Prolomit celou šifru se mu však zatím nepodařilo. V roce 2014 o tom informoval na svých stránkách. [cit. 31. 5. 2017]. Dostupné z: `http://scienceblogs.de/klausis-krypto-kolumne/2014/05/23/die-ungeloeste-geheimschrift-von-kaiser-ferdinand-iii/`.

[42] Srov. program konference [online]. [cit. 31. 5. 2017]. Dostupné z: `https://www.uni-erfurt.de/fileadmin/user-docs/FGE/Veranstaltungen_2013/Tagungen/Geheime_Post/Flyer_Geheime_Post.pdf`.

[43] ROUS, Anne-Simone - MULSOW, Martin. *Geheime Post: Kryptologie und Steganographie der diplomatischen Korrespondenz europäischer Höfe während der Frühen Neuzeit.* Berlin: Duncker & Humblot, 2015.

[44] Není bez zajímavosti, že heslo „Dechiffrování“ v Riegrově slovníku naučném je dílem právě A. V. Malocha. Srov. Kašpar, J. *Soubor statí*, s. 181.

[45] MALOCH, Antonín Vánkomil. *Rozluštění chiffrovaného písma v češtině.* In: Lumír, 1858, roč. 8, č. 9, s. 205-206. Zde také cituje Václava Hanku, který zbylé dopisy dešifroval pomocí přiložených klíčů. Zmíněnému českému lístku jako jedinému klíč chyběl.

obsah, avšak nezmínil se ani o šifře samotné, ani o způsobu rozluštění.

První českou prací, zabývající se šifrováním v teoretické rovině, je populárně naučná příručka *Jaromíra Lichtnera.*[46] Na začátku se v krátkosti věnuje metodám utajení textu pomocí sympatetických inkoustů a následně popisuje jednotlivé typy šifer, aniž by však uvedl literaturu, z níž čerpal. Byl však první, kdo vytvořil základní českou kryptologickou terminologii, která u nás do té doby zcela chyběla, v čemž vidí Jaroslav Kašpar největší přínos této příručky.[47] Je třeba ale podotknout, že ne všechny Lichtnerem užité termíny se ujaly.[48]

Šifrám coby konkrétním historickým pramenům u nás větší pozornost věnovali *František Roubík* a *Anna Vavroušková.* Prvně jmenovaný rozluštil šifrované dopisy, uložené v registratuře Albrechta z Valdštejna. V krátké studii je rozdělil do skupin podle jednotlivých šifrovacích klíčů, které otiskl a stručně popsal.[49] V citované práci se nezabývá obsahem dopisů, avšak přepisy šifrovaných částí poskytl tehdejšímu Archivu ministerstva vnitra, který je zařadil k písemnostem Valdštejnovy vojenské kanceláře.[50] Předmětem zájmu Anny Vavrouškové byly tři šifrované dopisy Fridricha Falckého nizozemským generálním stavům a Mořici Oranžskému, pro něž bylo užito jednoho šifrovacího klíče.[51]

O tajném písmu, které měli užívat povstalci ve vzájemné korespondenci během selského povstání roku 1775, informoval *Václav Husa.* V článku ocitoval prameny, které se o této skutečnosti zmiňují. K tomu jsou přímo otisknuty i dva klíče. Autor však nenalezl žádné šifrované dopisy.[52] K šifrování v době středověku pak existuje krátký článek *Bohumila Ryby.*[53]

Největší pozornost tajným písmům věnoval již zmiňovaný *Jaroslav Kašpar.* V *Příspěvku k řešení tajného písma ze 17. století* popisuje princip rozluštění soukromých šifrovaných dopisů vévodkyně Anny Magdaleny Sasko-Lauenburské, utajených jednoduchou substituční šifrou. Později publikoval v *Souboru statí o novověkém písmu* obecné pojednání o šifrování v novověku, koncipované jako seznámení historiků a archivářů se šifrovacími systémy a způsoby jejich luštění pro

[46] LICHTNER, Jaromír. *Šifrování. Úvod do kryptografie chemické i grafické se 40 šifrovými klíči.* Praha: Alois Srdce, 1939.

[47] KAŠPAR, J. *Soubor statí*, s. 181.

[48] Tak například jím užité slovo „maska“ pro šifrové znaky bez významu se dnes označuje spíše slovem „klamač“ či „bludička“. Srov. KAŠPAR, J. *Příspěvek k řešení tajného písma*, s. 98; MÍRKA, J. *Raně novověká šifrovaná korespondence*, s. 47.

[49] ROUBÍK, František. *Šifrované dopisy v registratuře Albrechta z Valdštejna.* In: Sborník prací věnovaných prof. dru Gustavu Friedrichovi k šedesátým narozeninám: 1871-1931. Praha: Historický spolek v Praze, 1931, s. 359-368.

[50] Tamtéž, s. 368.

[51] VAVROUŠKOVÁ, Anna. *Šifrované dopisy Fridricha Falckého.* Praha: [s.n.], 1933.

[52] HUSA, Václav. *K dějinám nevolnického povstání roku 1775.* In: Český lid, 1952, roč. 39, č. 11-12, str. 243-255.

[53] RYBA, Bohumil. *K tajnému písmu v listech Husových.* In: Sborník historický 1, 1953, s. 46-52.

praktické využití při práci se zašifrovanými prameny.[54] V obou pracích také jako první uvedl zahraniční a domácí literaturu k šifrování. Šiframi raně novověkých pramenů v českých archivech se dnes zabývá *Jakub Mírka*, jehož článek je rozebrán výše.

[54] Srov. KAŠPAR, J. *Soubor statí*, s. 178-180.

2. Základní terminologie ke kryptologii

Ve starších českých pracích historiků a archivářů, které se týkající šifrování, není odpovídající terminologie nijak ustálena. Zmiňovaná kryptografická příručka Jaromíra Lichtnera sice zavedla určité pojmy, z nichž se některé později ujaly, avšak mnohým jevům vhodná pojmenování stále chyběla. Názvosloví, které lze použít i v historicky zaměřené práci o šifrování, vytvořili v současné době čeští kryptologové. Pro účely této práce byly užity převážně základní pojmy, definované v první kapitole populárně naučné knihy o metodách a historii šifrování kryptologa Pavla Vondrušky.[55]

2.1 Základní definice

Utajené zprávy lze obecně zkoumat ze dvou různých pohledů: *kryptografie* či *kryptoanalýzy*. Kryptografie se dále dělí na *klasickou* a *moderní*. Předmětem klasické kryptografie byly metody šifrování, které sloužily ke skrytí obsahu zprávy před nepovolaným čtenářem. Jednalo se zejména o jednodušší šifrovací systémy, které se dnes označují jako historické šifrovací systémy.[56] Sem tedy patří téma této práce. Moderní kryptografie se zrodila po druhé světové válce. Dnešní složité systémy utajování předávaných informací vychází ze znalostí matematiky a informatiky.[57] Luštěním utajených zpráv, často za účelem prolomení celého šifrovacího systému, se zabývá kryptoanalýza. Zde je nutné uvést dva pojmy, které v naší starší odborné literatuře nebyly rozlišovány: *dešifrování* a *luštění*. V prvním případě se jedná o převedení zašifrovaného textu do původní podoby na základě znalosti šifrovacího klíče. Naproti tomu luštěním se rozumí činnost, kdy se kryptoanalytik snaží prolomit šifru bez znalosti klíče.[58] Věda, která obě uvedené disciplíny spojuje, se souhrnně nazývá *kryptologie*. Někdy k ní bývá řazena i *steganografie*, jejímž cílem je zastřít samotnou skutečnost, že se jedná o předávanou zprávu. U takto utajené zprávy se někdy hovoří o *skrytém tajném písmu*.[59]

[55] VONDRUŠKA, P. *Kryptologie*, s. 8-35. Další odkazy budou uvedeny jen v případě čerpání příslušné informace z jiného zdroje.

[56] KLÍMA, V. *Základy moderní kryptologie*, s. 3.

[57] Tamtéž.

[58] V našem prostředí se donedávna užívalo pro obě činnosti pojmu „dešifrování“. Srov. KAŠPAR, J. *Soubor statí*, s. 192. Např. v němčině se oba výrazy rozlišovaly již dříve. Pojmy „entschlüsseln“ pro dešifrování a „entziffern“ pro luštění uvádí například Erich Hüttenhain ve své práci z roku 1974. Srov. HÜTTENHAIN, E. *Die Geheimschriften*, s. 13.

[59] KAŠPAR, J. *Soubor statí*, s. 182. Utajení existence zprávy lze provést buď pomocí chemických reakcí (např. neviditelné inkousty), nebo skrytím zprávy v jiném textu či obrázku.

Zpráva se ve své čitelné, srozumitelné podobě označuje jako *otevřený text*. Její zašifrované verzi se říká *šifrový text*, případně *šifrát*.[60] V prvém případě označujeme jednotlivé elementy zprávy jako *znaky* či *abecedu* otevřeného textu. Šifrový text může v závislosti na použitém typu šifrovacího systému obsahovat jak znaky otevřeného textu, tak znaky *šifrové abecedy*.

2.2 Typy šifrovacích systémů

Základní rozdělení klasických šifrovacích systémů rozlišuje *transpoziční* a *substituční* systém a šifrování pomocí *kódové knihy*.

Transpozicí se rozumí přemístění jednotlivých znaků otevřeného textu na jiné pozice ve zprávě pomocí určitých pravidel. Za nejjednodušší varianty lze považovat přesmyčky (*anagramy*) či vytvoření geometrického obrazce, v němž se písmena zprávy čtou v určitém jeho směru. Složitější formou je přeskupování písmen podle číselného klíče. Pro zvýšení bezpečnosti mohla být písmena šifrového textu následně ještě rozdělena do skupin nebo uspořádána do obrazců. Dalším typem transpoziční šifry je použití *šifrovací mřížky*, v níž se některá políčka vyřízla. Po přiložení mřížky na papír se do volných políček vepsala písmena zprávy. Prázdná místa byla po odejmutí mřížky doplněna náhodnými písmeny. Dokonalejší variantou je pak čtvercová *otočná mřížka*, v níž se vyřízla právě čtvrtina políček. Mřížka se po zaplnění vystřižených políček postupně otáčela o 90°, tedy celkem čtyřikrát. Při správném sestavení mřížky bylo po posledním otočení zaplněno všech n^2 políček a na každé políčko připadlo právě jedno písmeno.[61]

Při šifrování substituční metodou dochází k záměně znaků otevřeného textu za znaky šifrové abecedy. Těmito znaky mohou být číslice, nejrůznější symboly, znaky jiného jazyka nebo i znaky otevřeného textu, které však v šifrátu mají, na rozdíl od šifrového textu vzniklého pomocí transpozice, odlišný význam. Nahrazeno může být jednotlivé písmeno, dvojice sousedních písmen (*bigram*), případně tři (*trigram*) či více po sobě jdoucích písmen (*polygram*). Substituční šifra, v níž je jeden znak otevřeného textu nahrazen právě jedním šifrovým znakem a zároveň je pro celé sdělení užito stejné šifrové abecedy, se nazývá *jednoduchá substituce* nebo také *monoalfabetická šifra*. Při jejím použití zůstává četnost šifrových znaků v šifrátu shodná s četností jim odpovídajících znaků otevřeného textu. To je také slabinou této šifry, umožňující u dostatečně dlouhého textu zprávu snadno rozluštit. Postup luštění, vycházející ze zkoumání různé četnosti hlásek daného jazyka se označuje jako *frekvenční analýza*. Uvedený nedostatek samozřejmě vyvolával

Opačným pojmem pak je *zjevné tajné písmo*, u něhož je zřejmě, že se jedná o zašifrovanou zprávu.

[60] Tamtéž.

[61] Tamtéž, s. 183-186; KLÍMA, V. *Utajené komunikace*, s. 120.

snahy po zkreslení četnosti. Jedním z možných opatření bylo užívání šifrových znaků bez významu. Ty se nazývají *klamače* či *bludičky*.[62] V otevřeném textu nemají žádný ekvivalent.

Další variantou ztížení luštění bylo jisté zdokonalení jednoduché substituce tím, že se některým znakům otevřeného textu (typicky těm nejčastěji užívaným, tedy např. samohláskám) přiřadilo více znaků šifrové abecedy. Tomuto typu šifry se říká *homofonní substituce*.[63] Ani tuto šifru nelze považovat za bezpečnou. Stále jsou v ní zachovány jisté pravidelnosti (například bigramové vazby), které lze objevit u delšího textu. Homofonní šifry stejně jako jednoduché substituce užívají pouze jedné šifrové abecedy. V případě šifrování jednoho textu substituční metodou za použití více šifrových abeced hovoříme o *polyalfabetické substituci*.

Nahrazována mohou být i celá slova, jejichž šifrové znaky se v šifrovém textu označují jako *kódy*.[64] V principu se tedy jedná o substituci,[65] avšak šifrování pomocí kódů je považováno za třetí základní šifrovací systém vedle transpozice a substituce. Ze seznamů kódů, které kromě slov nahrazovaly i věty a souvětí, později vznikaly *kódové knihy*. Jejich předchůdcem je tzv. *nomenklátor*, který byl hojně užívanou šifrovací technikou v době raného novověku. Jednoduché nomenklátory se skládaly z monoalfabetické či homofonní šifry a několika kódů pro často užívaná slova příslušné korespondence nebo například pro vlastní jména. Propracovanější nomenklátory pak kromě většího počtu kódů obsahovaly i šifrové znaky pro slabiky, bigramy, trigramy či klamače.[66]

[62] KAŠPAR, J. *Soubor statí*, s. 187. V šifrovacích klíčích z doby raného novověku je lze poznat podle označení „errantes“ nebo „nullae“. Srov. MÍRKA, J. *Raně novověká šifrovaná korespondence*, s. 47.

[63] Homofony – šifrové znaky odlišné podoby, ale shodného významu v otevřeném textu.

[64] Klasický význam slova „kód“ se od svého významu v kryptologii liší. Kód převádí zprávu do podoby, kdy ji lze přenášet či jinak technicky zpracovat. Příkladem takového kódu je např. Morseova abeceda. Smyslem zakódované zprávy tedy není skrytí jejího obsahu, čímž se kód v původním slova smyslu liší od šifry. Naproti tomu v kódových knihách není význam jednotlivých kódů všeobecně znám, nýbrž záměrně utajen. Proto se jedná o šifrovací systém.

[65] MÍRKA, J. *Raně novověká šifrovaná korespondence*, s. 47.

[66] VONDRUŠKA, P. *Šifrování*, s. 210, 234.

3. Matyáš Gallas na pozadí třicetileté války

Matyáš Gallas se narodil 17. října roku 1588[67] v tridentské šlechtické rodině. Starobylý ministeriální rod, z něhož Gallas pocházel, je spojen s držbou hradu Campo, podle něhož rodina získala své jméno. Matyáš Gallas byl proto uváděn jako hrabě z Kampu, ačkoli už od 15. století hrad rodině fakticky nenáležel.[68]

Životní osudy Matyáše Gallase před třicetiletou válku jsou pro nedostatek pramenů těžko uchopitelné. Patrně už v raném mládí se rozhodl pro dráhu profesionálního vojáka, kterým byl i jeho otec Pankrác. Jako páže byl Gallas poslán do Lotrinska ke dvoru Ferdinanda Madruzza, svobodného pána z Bauffremontu, v jehož službách později započala Gallasova vojenská kariéra, kdy se v hodnosti praporčíka a posléze poručíka zúčastnil španělsko-piemontské války. Roku 1618 ho tridentský biskup ustanovil hejtmanem v Rivě. Jeho hejtmanství se však od počátku neslo ve znamení neshod tridentského biskupa s tyrolskou vládou, která biskupovi vytýkala porušení práv při jmenování Gallase do funkce, v níž přesto nakonec setrval až do začátku roku 1621.[69]

Tehdy na post hejtmana v Rivě rezignoval a odešel do Bavorska, aby se připojil k vojskům Katolické ligy, která se pod vedením vévody Maxmiliána I. přidala na počátku třicetileté války na stranu císaře Ferdinanda II. V ligistickém vojsku sloužil Gallas nejprve jako nejvyšší strážmistr a zástupce Jana Jakuba z Bronckhorstu a Anholtu. Po svém vstupu do Ligy byl odvelen do Horních Rakous, které se staly dočasnou bavorskou zástavou. Zanedlouho však stanul na bojišti na německé půdě, kam se přesunulo ohnisko bojů po porážce českého stavovského povstání. V bojích se projevil jako schopný voják, za což se dočkal dalších povýšení, a to do hodností poručíka a záhy plukovníka. V srpnu roku 1623 si vysloužil uznání za svůj podíl na vítězství vojsk Katolické ligy v bitvě u Stadtlohnu, kde generál poručík Tilly definitivně porazil Kristiána Brunšvicko-Wolfenbüttelského. O dva roky později se plukovník Gallas stal majitelem svého pluku. Přestože bojoval pod praporem Ligy úspěšně i nadále, o čemž svědčí například opakovaná Tillyho snaha o Gallasovo povýšení na generál strážmistra, této hodnosti v Ka-

[67] V odborné literatuře je dodnes uváděno chybné datum 16. září 1584, přestože na základě matriky křtů tridentského farního kostela sv. Petra bylo dokázáno Gallasovo skutečné datum narození, které vzal např. italský historik René Preve Ceccon na vědomí už v roce 1990. Zápis v tridentské matrice křtů ze 16. září 1584 patří Gallasovu stejnojmennému bratrovi, který zemřel brzy po narození a po němž byl Matyáš Gallas pojmenován. Srov. REBITSCH, R. *Matyáš Gallas*, s. 30-31, 251.

[68] Tamtéž, s. 28.

[69] Tamtéž, s. 31-33; KILIÁN, Jan. *Jan Matyáš Gallas*. In: Valdštejn: Albrecht z Valdštejna Inter arma silent musae?. Praha: Academia, 2007, s. 287.

tolické lize nedosáhl. Roku 1629 přijal nabídku generálského postu od Albrechta z Valdštejna, který usiloval o získání Gallase do císařské armády.[70]

Čerstvý generál strážmistr císařských vojsk svoji kariéru pod Ferdinandem II. započal v Itálii ve válce o mantovské dědictví. Jednalo se o konflikt, jenž vznikl po vymření hlavní linie rodu Gonzagů, kteří drželi Mantovu. O ni se ihned přihlásil Karel z Nevers z vedlejší gonzagovské větve, za kterého se postavila Francie. Španělsko však usilovalo o prosazení kandidáta z jiné vedlejší větve Gonzagů a potažmo o udržení Itálie mimo francouzskou sféru vlivu. Španělsko se obrátilo o pomoc k císaři jakožto lennímu pánovi.[71] Císař nakonec poslal do Mantovy armádu, jejímž velitelem se stal generál poručík hrabě Collalto. Tomu byli coby zástupci přiděleni generálové Matyáš Gallas s Janem Aldringenem. Ti se pak po Collaltově smrti roku 1630 stali oficiálními veliteli císařských sborů v Itálii. Gallasovi se v Itálii vojensky dařilo. Porazil kupříkladu Benátčany, spojence Neverse, a přispěl i k pádu samotné Mantovy, která byla poté vypleněna. Uplatnil se zde i jako diplomat během mírových jednání s Francií. Jeho diplomatický počin vyzdvihl císař při povýšení Gallase do hraběcího stavu.[72]

Zpět do Říše se Gallas vrátil na podzim roku 1631. Když byl pak v prosinci téhož roku povolán Valdštejn opět k vrchnímu velení císařské armády, jedna z prvních věcí, kterou po svém návratu učinil, bylo zajištění povýšení Matyáše Gallase.[73] Ten od této doby sloužil jako generál císařský zbrojmistr a jeden z nejdůležitějších Valdštejnových důstojníků, kterému také generalissimus jako veliteli nechával značnou míru samostatnosti. Po znovu sestavení císařské armády na jaře roku 1632 se Gallas podílel na vytlačení Sasů z Českého království, se svým sborem poté pomohl u Norimberku proti Švédům a následně byl odvelen do Saska, kde si vysloužil povýšení do hodnosti polního maršála. Po bitvě u Lützenu, které se Gallas neúčastnil, byl poslán do Slezska, aby tam reorganizoval druhý hlavní císařský kontingent. Ačkoli se ve Slezsku na jaře roku 1633 Gallasova armáda spojila s armádou Valdštejnovou, generalissimus této síly k ofenzivě nevyužil. Soustředil se spíše na jednání s nepřátelskou stranou, což vyvolalo u císařského dvora nelibost. Gallas byl do Valdštejnových neprůhledných plánů zasvěcen. O důvěře, kterou k němu Valdštejn choval, koneckonců vypovídá i jeho návrh na Gallasovo povýšení do hodnosti generál poručíka. Císař žádosti vyhověl, čímž se Gallas stal po Valdštejnovi druhým mužem v císařské armádě.[74]

Když upadl Valdštejn v nemilost a ve Vídni padlo rozhodnutí o jeho osudu, zůstal Gallas loajální habsburské dynastii. V konečném důsledku měl navíc podíl

[70] REBITSCH, R. *Matyáš Gallas*, s. 34-39; KILIÁN, J. *Jan Matyáš Gallas*, s. 288.
[71] Mantova byla říšským lénem. Srov. REBISTCH, R. *Matyáš Gallas*, s. 42.
[72] Tamtéž, s. 42-50.
[73] KILIÁN, J. *Jan Matyáš Gallas*, s. 289.
[74] REBITSCH, R. *Matyáš Gallas*, s. 52-58.

na exekuci frýdlantského vévody. V lednu 1634, když císař Ferdinand II. Valdštejna podruhé a tentokrát definitivně sesadil z vrchního velení, byl totiž dočasným vrchním velitelem císařských vojsk jmenován právě Matyáš Gallas. Ačkoli se chebských událostí osobně neúčastnil, zodpovědnost za vykonání císařova příkazu, aby byl Valdštejn zajat nebo zabit, leží hlavně na něm. Po smrti svého někdejšího velitele, jemuž Gallas vděčil za svůj vojenský vzestup, získal tridentský rodák Valdštejnovo frýdlantské panství, což ho zařadilo mezi největší pozemkové vlastníky v českých zemích.[75]

V dubnu 1634 ztratil Gallas post vrchního velitele císařských vojsk, protože tato funkce byla přenesena na Ferdinanda III., budoucího císaře, v té době zatím českého a uherského krále. Gallas byl ale od toho okamžiku prvním důstojníkem a navíc byl ustaven jako Ferdinandův vojenský poradce.[76]

Letní ofenziva toho roku směřovala proti Bernardu Výmarskému a Švédům. Císařská armáda dobyla Řezno a Donauwörth. Poté císařští pokračovali k Nördlingenu, kde se 5.-6. září střetli se spojenou švédsko-výmarskou armádou. Početně silnější císařská armáda, doplněná o bavorské a španělské síly, pod vedením Matyáše Gallase, kterému Ferdinand III. oficiálně svěřil vrchní velení po dobu bitvy, zaznamenala triumfální vítězství. Gallas se ocitl na vrcholu své vojenské kariéry. Bitva u Nördlingenu byla ale zároveň jeho poslední otevřenou bitvou. Nadále vedl již jen defenzivní způsob boje.[77]

V roce 1635 vypověděla Francie válku Španělsku, kterému na pomoc přišla císařská armáda. Ta se v říjnu spojila proti francouzským vojskům s vévodou Karlem Lotrinským, velitelem bavorské armády, avšak k nelibosti lotrinského vévody Gallas žádný střet nepodnikl, nýbrž přešel do defenzivy. Tažení proti Francii se tedy uskutečnilo až následujícího roku,[78] kdy císařská armáda vpadla pod vedením Gallase do Burgundska a pokusila se o dobytí jeho hlavního města Dijonu. Před Dijonem se však Gallas s armádou obrátil k městečku Saint-Jean-de-Losne, ovšem po neúspěšných pokusech o jeho dobytí tažení proti Francii prakticky skončilo. Kvůli vytrvalým dešťům, které se podepsaly na stavu cest, musel navíc před městem zanechat část dělostřelectva. Nezdary let 1635 a zejména 1636 mu později vysloužily nelichotivou přezdívku „kazivoj“.[79]

V době císařského tažení proti Francii roku 1636 se na říšské půdě znovu objevili Švédové v čele s polním maršálem Janem Banérem. Část císařské armády byla ponechána k dispozici Španělsku, s větší částí se odebral Gallas do Saska, kde se

[75] Tamtéž, s. 61-62, 68.
[76] Tamtéž, s. 73.
[77] Tamtéž, s. 77-78, 80.
[78] Tamtéž, s. 83, 91.
[79] Tamtéž, s. 103-105, 124.

měl vypořádat se Švédy. Protože se mezitím stal Ferdinand III. císařem,[80] a nemohl tedy nadále působit přímo na bojišti, bylo svěřeno vrchní velení Gallasovi.[81] Ten zahájil rychlé pronásledování Banéra, kterého úspěšně vytlačoval z Říše severním směrem, až nakonec Banérovi zůstala pouze možnost úniku do Pomořan. Byl ovšem císařskou armádou zablokován a z pasti se dostal až pomocí lsti. Gallasovi se ale podařilo obsadit část Pomořan a Meklenburska, a to i přesto, že část jeho armády byla odvelena do bojů proti Francii.

Boji vyčerpané území však nedokázalo zajistit zásoby. Dalším problémem pro Gallasovu armádu se ukázalo zimní přezimování, k čemuž severoněmecká města nebyla ochotná. Na jaře 1638 se armáda nacházela ve velmi špatném stavu. Navíc musel Gallas postoupit další části svého sboru pro jiné operace v Říši. Opačně ale situace vypadala na švédské straně. Banér byl zásobován po moři ze Švédska a s finanční pomocí Francie dokázal regenerovat a posílit armádu. Pod svoji kontrolu znovu získával Pomořany a Meklenbursko. Na přelomu let 1638 a 1639 pro Gallase neúspěšné tažení skončilo. Banér pokračoval dál k jihu, do Saska a nakonec do Čech, kde stanul před Prahou. Tu se sice podařilo ubránit, ale zároveň už bylo rozhodnuto o výměně vrchního velení. Matyáš Gallas z postu rezignoval, oficiálně ze zdravotních důvodů, a byl poslán do výslužby. Na jeho místo nastoupil císařův bratr, arcivévodova Leopold Vilém.[82]

Pod novým vrchním velitelem se podařilo vytlačit Švédy z Čech. Po smrti Banéra ale v čele švédské armády stanul neméně schopný vojevůdce Lennart Torstensson, který roku 1642 císařským uštědřil porážku u Breitenfeldu. Krátce poté Leopold Vilém abdikoval a do čela císařské armády se vrátil Gallas, do té doby pobývající v Tridentsku. Na jaře roku 1643 Švédové opět pronikli do Čech. Zdálo se, že Torstensson míří k Praze. Jeho cílem však nebylo napadnout hlavní město, proto se stočil na Moravu. Gallas zachovával defenzivní způsob boje, čímž umožnil Torstenssonovi bezproblémový průchod. Pak už švédský generál získával jedno město za druhým. Na podzim se však Torstensson nečekaně stáhl, protože dostal rozkaz vrátit se na sever, kde začala válka Švédska proti Dánsku.[83]

Císař přislíbil dánskému králi pomoc. V květnu roku 1644 byla proto armáda v čele s Gallasem poslána na tažení do Holštýnska. Když císařští konečně dorazili do holštýnského vévodství, obsadili město Kiel, od čehož si Gallas sliboval zablokování Torstenssonovy armády ve Šlesvicku-Holštýnsku. To se ukázalo jako chybný předpoklad, neboť Torstensson na Gallase v Kielu nereagoval a zahájil postup směrem na habsburské dědičné země. Císařská armáda se dala na ústup z Kielu. Ačkoli se při pronásledování Švédů ocitly obě armády paralelně vedle

[80] V únoru 1637.
[81] REBITSCH, R. *Matyáš Gallas*, s. 111-115.
[82] Tamtéž, s. 117-136.
[83] KILIÁN, J. *Jan Matyáš Gallas*, s. 293.

sebe, došlo pouze k menším šarvátkám. Navíc se vojsko začalo pomalu rozpadat vlivem dezerce, nemocí a špatného zásobování. Vrchní velitel začínal propadat zoufalství. Gallasovi se přesto podařilo dostat se v září do města Bernburg a obnovit kázeň ve vlastní armádě. S příchodem Švédů se ale problémy brzy vrátily, protože Torstensson hodlal nechat město vyhladovět. S úderem zimy se císařská armáda ocitla v naprosto neutěšeném stavu. Gallas se ještě zvládl dostat s armádou k Magdeburku, kde doufal v proviant pro svoje vojáky, ale velitel města vojsko ani nevpustil dovnitř. V prosinci už situace vypadala katastroficky, když se vojsko rapidně ztenčilo dezercemi a úmrtím vojáků v důsledku hladu, zimy a chorob. Když město konečně dostalo rozkaz k otevření bran, zůstal Gallas s nemocnými, zatímco pochodu schopný zbytek vojska byl poslán do Prahy. Se zotavenou částí armády se později vrátil i Gallas, a to v únoru 1645. Ačkoli mu císař katastrofální tažení nevyčítal, nahradil jej ve vrchním velení opět Leopold Vilém.[84]

Tentokrát ale Gallas u armády setrval jako generál poručík. Roku 1646 se však natolik zhoršil jeho zdravotní stav, že musel být postaven mimo službu. Leopold Vilém toho roku podnikl neúspěšné tažení do Vestfálska, aby zabránil spojení Švédů a Francouzů. Arcivévoda poté požádal o uvolnění z funkce a vrchním velitelem se naposledy ve své kariéře v prosinci roku 1646 stal Matyáš Gallas. Třetí a poslední generalát však trval jen čtyři měsíce, jejichž náplní bylo převážně jednání s bavorským kurfiřtem, který uvažoval o separátním míru se Švédy a Francií. Z důvodu vážného zdravotního stavu bylo 17. dubna 1647 Gallasovi odejmuto vrchní velení. Osm dní poté Matyáš Gallas zemřel.[85]

Přestože ne všichni Gallasovi současníci hodnotili generál poručíka kritickými slovy, vešel do dějin jako na alkoholu závislý[86] „kazivoj“, který *„dokáže zruinovat celé armády“*.[87] Ačkoli lze i v moderní historiografii nalézt pozitivní či o objektivitu se snažící hodnocení tridentského rodáka, zůstal Gallas až donedávna ve stínu své nelichotivé pověsti. Roku 2006 se však dočkal svojí první opravdové monografie z pera rakouského historika Roberta Rebitsche, která se snaží o *„diferencovaný obraz generál poručíka“*[88] a z jejíhož českého překladu bylo převážně čerpáno pro tuto kapitolu.

[84] REBITSCH, R. *Matyáš Gallas*, 154-174.
[85] Tamtéž, s. 185-203.
[86] Tamtéž, s. 15.
[87] Tamtéž, s. 22.
[88] Tamtéž, s. 14.

4. Analýza šifrované korespondence Gallasovy válečné kanceláře

Válečná kancelář Matyáše Gallase je uložena ve fondu Historická sbírka Clam-Gallasů pod inventárním číslem 1397. Celkově čítá asi 7 500 písemností[89] z let 1627-1648.[90] Z celkového počtu 50 kartonů jich 48 připadá na chronologicky řazené dokumenty válečné kanceláře.[91] V jednom kartonu je uložena abecedně uspořádaná kartotéka korespondentů Matyáše Gallase.[92] Na většině záznamů je uvedeno jméno a titulatura adresáta s následným výčtem jeho dopisů, které se v registratuře nacházejí. Z některých zápisů lze dokonce zjistit i podrobnější informace o konkrétním dopisu, včetně toho, je-li šifrován. Ne všechny záznamy jsou ale detailněji rozepsány, takže se v tomto ohledu nelze spolehnout pouze na kartotéku. Poslední karton obsahuje soubor šifrovaných dopisů a klíčů z let 1637-1644, dopisy od Baltasara Marradase a složku nedatovaných zpráv, memoriálů, dobrozdání, instrukcí a korespondence od jednotlivých osob a měst.[93]

4.1 Podíl šifrované korespondence v rámci válečné kanceláře

Na základě zkoumání všech písemností válečné kanceláře jsem zjistila, že je v ní dochováno celkem 201 šifrovaných písemností. Do tohoto počtu je zahrnuta každá jednotlivá písemnost, jejíž obsah je úplně, nebo jen částečně zašifrován. V případě, že šifrovaný dokument existuje v několika vyhotoveních, je započítán jednou. Kromě uvedeného souboru šifrovaných dopisů a klíčů, který je tvořen devíti šifrovanými dopisy, jedenácti dochovanými šifrovacími klíči a několika dešifrovanými otevřenými texty, je zbylých 192 šifrovaných dopisů zařazeno v registratuře mezi ostatními (nešifrovanými) písemnostmi. Složka šifrovaných dopisů byla během pořádání fondu vytvořena patrně náhodným výběrem, protože s největší pravděpodobností dopisy v ní uložené spolu nijak nesouvisí a až na jeden z nich

[89] POLIŠENSKÝ, Josef (edd). *Documenta Bohemica bellum tricennale illustrantia. Tomus I.*, Praha: Academia, 1971, s. 214.

[90] Samotná korespondence je vedena do roku 1647. Pro léta 1647-1648 jsou pak dochovány účty dvorského ubytovatele. Srov. SMÍŠKOVÁ, H. *Inventář*, s. 79-81.

[91] SOA v Litoměřicích – pobočka Děčín, Historická sbírka (rodinný archiv) Clam-Gallasů, Frýdlant, inv. č. 1397, sign. XVIII/1 – XV/18, kart. 343–390.

[92] Tamtéž, sign. XV/19, kart. 391.

[93] Tamtéž, sign. XV/20, kart. 392.

na ně ani nelze použít žádný z přiložených šifrovacích klíčů. Také dešifrované texty ve všech případech neodpovídají příslušným dopisům.[94]

Podíl šifrované korespondence Gallasovy válečné kanceláře činí asi 2,68 % všech písemností. Vzhledem k předpokladu, že kancelář zůstala dochována v úplnosti,[95] můžeme údaj považovat za relevantní. Ačkoli celkový nárůst počtu písemností Gallasovy válečné kanceláře lze pozorovat už od roku 1633,[96] šifrovaná korespondence se v registratuře poprvé objevuje až roku 1634, což je v Gallasově vojenské kariéře rok velmi významný. Generál poručík se stal provizorním vrchním velitelem císařských vojsk a ačkoli vrchní velení bylo nedlouho po Gallasově jmenování oficiálně přeneseno na následníka trůnu Ferdinanda III., zůstal Gallas prvním důstojníkem v císařské armádě. Komunikaci prostřednictvím šifrovaných zpráv vedl Gallas s různou intenzitou po celou dobu svého prvního generalátu, tedy do roku 1639, ačkoli z tohoto roku existuje jen jedno šifrované psaní, a sice originál dopisu císaře Ferdinanda III. adresovaného ale nikoli Gallasovi, nýbrž Jindřichu Šlikovi, prezidentovi dvorské válečné rady.[97] Celkem se pro toto šestileté období nachází v registratuře 52 šifrovaných písemností. To je asi 25,87 % celé šifrované korespondence.

V letech 1640 – 1642 žil Matyáš Gallas ve výslužbě na svých tridentských statcích, což se odráží i v jeho vojenské kanceláři, která je v této době „zcela bezobsažná.“[98] Není proto překvapivé, že z uvedených let neexistuje žádný šifrovaný dopis. To se mění s opětovným jmenováním Gallase do čela císařské armády roku 1643, čímž započal jeho druhý generalát, trvající do roku 1645.[99] Do tohoto období spadá zbývajících 149 šifrovaných písemností, tedy zhruba 74,13 % veškerých dochovaných šifrovaných zpráv. Ačkoli byl koncem roku 1646 Matyáš Gallas ještě potřetí ve své kariéře povolán k vrchnímu velení, není korespondence z tohoto období příliš četná[100] a neobsahuje žádné šifrované písemnosti.

Šifrovanou korespondenci v rámci Gallasovy válečné kanceláře lze tedy rozdělit na období jeho prvního a druhého generalátu. Poměr v podílu šifrované korespondence v obou obdobích byl objasněn výše. Počet šifrovaných písemností v jednotlivých letech zobrazuje graf na obrázku 4.1.1.

Vzhledem k prostředí a době by mohlo být zajímavé srovnání podílu šifrované

[94] Ve zmiňované složce se například nachází dešifrovaný text dopisu císaře Ferdinanda III. Matyáši Gallasovi z 28. března 1637, zatímco samotný dopis je uložen mezi ostatními dokumenty z března toho roku. Srov. tamtéž, sign. XVIII/11, kart. 353.

[95] Srov. SMÍŠKOVÁ, H. *Inventář*, s. IV.

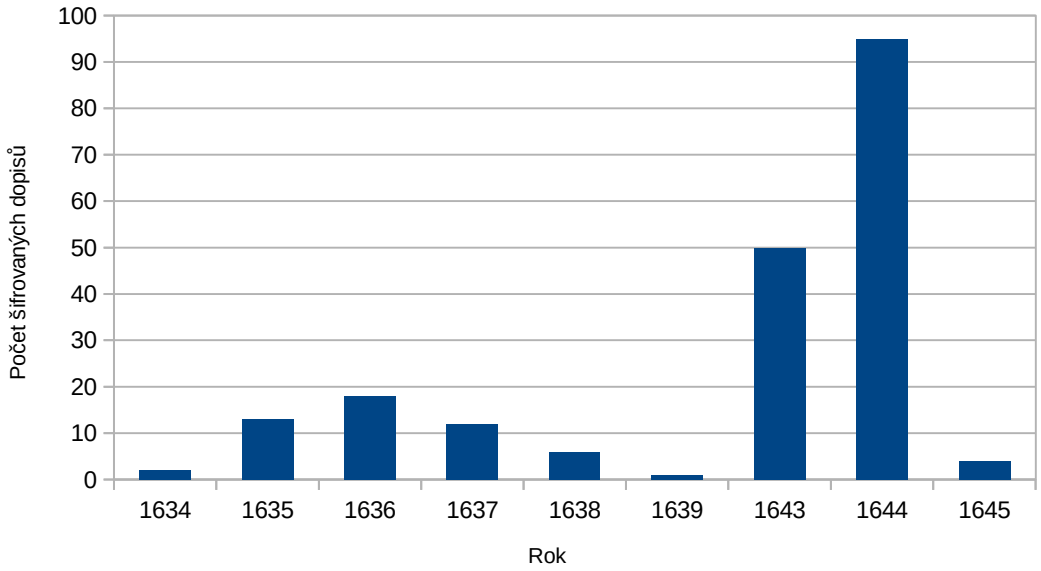
[96] Písemnosti let předchozích, tedy 1627-1632, jsou obsaženy v jediném kartonu. Pro srovnání, na samotný rok 1633 připadají dva kartony. Srov. tamtéž, s. 79.

[97] HS Clam-Gallasů, sign. XVIII/20, kart. 362.

[98] REBITSCH, R. *Matyáš Gallas*, s. 287.

[99] KILIÁN, J. *Jan Matyáš Gallas*, s. 293.

[100] Na každý z roků 1646 a 1647 připadá pouze jeden karton. Srov. SMÍŠKOVÁ, H. *Inventář*, s. 81.



Obrázek 4.1.1: Počet šifrovaných dopisů v jednotlivých letech.

korespondence válečné kanceláře Matyáše Gallase a registratur jiných vojevůdců třicetileté války. Takto prozkoumána již byla vojenská kancelář Gallasova „předchůdce“ Albrechta z Valdštejna. Ta dnes obsahuje asi 25 000 písemností, z nichž je 65 šifrovaných.[101] To je asi 0,26 % veškeré korespondence. Na rozdíl od Gallasovy kanceláře ale Valdštejnovu registraturu nejspíše postihly ztráty, a to už bezprostředně po jeho zavraždění.[102] Je proto pravděpodobné, že i některé šifrované dopisy ztrátám podlehly.[103] Proto by v tomto případě bylo srovnání podílu šifrované korespondence v obou kancelářích zavádějící.

Pro ucelenější obraz o Gallasově válečné kanceláři, nejen z hlediska podílu šifrované korespondence, ale zejména v souvislosti s obsahem dokumentů, bude při dalším bádání nutné zkoumat i Gallasovy dopisy uložené v jiných fondech. V jeho válečné kanceláři se totiž nachází jen dva šifrované dopisy, jejichž odesílatelem je on sám. Jedná se o listy z 23. a 25. září 1644 císaři Ferdinandovi III.,[104] které byly po svém vyhotovení znovu upravovány a zůstaly tak v registratuře jako rekoncepty. O tom, že i z jeho kanceláře odcházela šifrovaná psaní, dále svědčí i koncept z 15. listopadu 1644,[105] na němž je označena pasáž, která měla být v čistopisu zašifrována.

[101] ROUBÍK, F. *Šifrované dopisy v registratuře Albrechta z Valdštejna*, s. 359.
[102] REBITSCH, R. *Matyáš Gallas*, s. 68.
[103] ROUBÍK, F. *Šifrované dopisy v registratuře Albrechta z Valdštejna*, s. 359.
[104] HS Clam-Gallasů, sign. XV/11, kart. 383.
[105] Tamtéž, sign. XV/13, kart. 385.

4.2 Rozbor vybraných šifer

Všechny šifrované písemnosti, včetně stručného popisu, jsou uvedeny v příloze A.1. Pro podrobný rozbor byly vybrány šifry pěti korespondentů Matyáše Gallase. Rozebrán je rovněž případ zachycených dopisů nepřátelské strany.

4.2.1 Šifra Matyáše Gallase s císařem Ferdinandem III.

Jako generál císařských vojsk sloužil za třicetileté války Matyáš Gallas postupně pod dvěma císaři – Ferdinandem II. a Ferdinandem III. Ve válečné kanceláři je dochována korespondence s oběma panovníky. V případě Ferdinanda II. ale žádný z dopisů šifrovaný není, ačkoli i Ferdinand II., jak víme z registratury Albrechta z Valdštejna, výjimečně zprávy utajoval.[106]

Oproti tomu komunikace Matyáše Gallase s Ferdinandem III. pomocí šifrovaných zpráv je v rámci veškeré šifrované korespondence válečné kanceláře poměrně bohatá. Ferdinand III. adresoval Gallasovi celkem 56 šifrovaných dopisů. U sedmi z nich, označených v soupisu písemností pořadovými čísly 77, 85, 91, 93, 107, 125 a 142, je přiložena alespoň jedna další šifrovaná písemnost, jejíž obsah je utajen stejnou šifrou, kterou císař užíval ve vzájemné korespondenci s Gallasem v období jeho druhého generalátu. Jedná se celkově o 12 písemností. Dochovány máme také dva rekoncepty Gallasových šifrovaných dopisů Ferdinandovi III. Více než třetina šifrovaných dokumentů celé kanceláře tak připadá na korespondenci Gallase s císařem.

První šifrovaný dopis, který Gallasovi dorazil od Ferdinanda III., v té době krále českého, uherského a chorvatského, je datován dne 8. října roku 1635.[107] Šifrovací klíč se nedochoval, ale nad několika šifrovými znaky byly vepsány odpovídající znaky otevřeného textu a samotný dešifrovaný text byl navíc přiložen na zvláštním listu, takže jsem klíč mohla rekonstruovat (viz tabulka 4.2.1).

Jde o homofonní substituci, kdy jsou každému písmenu abecedy přiřazeny dva šifrové znaky. V hranatých závorkách jsou uvedeny homofony, které sice nebyly použity ani v citovaném dopisu, ani v žádném z dalších zkoumaných šifrových textů, ale bylo je možné odvodit na základě systematického uspořádání šifrových znaků. Téměř jistě sestává klíč pouze z 21 písmen. Ve všech zkoumaných šifrátech jsou totiž písmena *K*, *W* a *Y*[108] důsledně utajována jako *CH*, *VV* a *I*, přestože při dešifrování byla přepisována zpět do původní podoby.

Tato substituční šifra je použita ve všech deseti šifrovaných dopisech, které

[106] ROUBÍK, F. *Šifrované dopisy v registratuře Albrechta z Valdštejna*, s. 360.
[107] HS Clam-Gallasů, sign. XVIII/7, kart. 349.
[108] Písmena *J* a *U* se v jazykově německých textech 17. století běžně psala jako *I* a *V*, proto jejich absence v šifrovacím klíči není překvapivá.

A	=	30, 60	H	=	39, 69	Q	=	48, [88]
B	=	33, 63	I	=	40, 80	R	=	49, 89
C	=	34, 64	L	=	43, 83	S	=	50, 90
D	=	35, 65	M	=	44, 84	T	=	53, 93
E	=	36, 66	N	=	45, 85	V	=	54, 94
F	=	37, 67	O	=	46, 86	X	=	[55], [95]
G	=	38, 68	P	=	47, 87	Z	=	56, [96]

Tabulka 4.2.1: *Rekonstruovaný šifrovací klíč pro „královskou“ šifru*

poslal Ferdinand III. Gallasovi v letech 1635-1638. Určitou dobu tedy Ferdinand tuto šifru užíval i jako císař Svaté říše římské.[109] Po svém návratu k císařské armádě v roce 1643 musel ale Gallas obdržet nový šifrovací klíč, protože už v první šifrované zprávě od císaře, 17. června toho roku,[110] je nová šifra použita. Zůstala pak v platnosti minimálně po dva roky Gallasova druhého generalátu.[111] Změna šifry, kterou můžeme pozorovat v korespondenci Matyáše Gallase s Ferdinandem III., však nevypovídá o tom, kdy přestal císař původní šifru užívat úplně. Ta totiž nebyla určena výhradně pro komunikaci s Gallasem, což dokládá dochovaný originál císařova šifrovaného dopisu z 11. května 1639 Jindřichu Šlikovi, prezidentovi dvorské válečné rady.[112] Na druhé straně i Gallas užíval původní šifru i mimo korespondenci s Ferdinandem. Polní maršálek Rudolf von Tiefenbach poslal 31. prosince 1636 Gallasovi dopis s přáním k novému roku.[113] Zároveň v něm Gallasovi vyjádřil soustrast nad neutěšeným stavem císařské armády po podzimním neúspěšném tažení do Burgundska. Právě pasáž, v níž vyslovuje lítost, je zašifrována pomocí „Ferdinandovy“ homofonní substituce.

Na rozdíl od staré šifry mezi Ferdinandem III. a Matyášem Gallasem zůstal šifrovací klíč k nové šifře dochován. Je uložený ve sbírce klíčů. Na jeho reversu je přímo uvedeno, že se jedná o šifru s císařem a uherským a českým králem.[114] Jedná se o propracovanější nomenklátor, který se skládá z homofonní substituce a šifrových znaků pro bigramy, klamače a kódy (viz obr. A.2.1 Přílohy A.2). Samohlásky mohou být nahrazeny pěti různými šifrovými znaky, souhlásky dvěma. Jednotlivým bigramům, které jsou uspořádány ve 24 skupinách po pěti (ab, eb, ib, ob, ub; ac – uc; ad – ud; af – uf; ba – bu; ca – cu; da – du; fa – fu; ag – ug; al – ul; am – um; an – un; ga – gu; la – lu; ma – mu; na – nu; ap – up; ar – ur; as

[109] Císařem se stal Ferdinand III. v únoru roku 1637. Srov. REBITSCH, R. *Matyáš Gallas*, s. 230.

[110] HS Clam-Gallasů, sign. XVIII/27, kart. 369.

[111] Poslední šifrovaný dopis od císaře je datován 30. 12. 1644.

[112] HS Clam-Gallasů, sign. XVIII/20, kart. 362. Za pozornost zde stojí nešifrovaná věta, která je uvedena na vloženém listu dopisu pod šifrovaným textem: „dise sein die Alt[en] Ziffer mit Ihrer Ex[zellenz] Herr[n] G[ene]ral lie[u]t[nant]?“ Vzhledem k užitému titulu se nepochybně vztahuje na Gallase.

[113] Tamtéž, sign. XVIII/10, kart. 352.

[114] Tamtéž, sign. XV/20, kart. 392.

– us; at – ut; pa – pu; ra – ru; sa – su; ta – tu), je přiřazen jeden šifrový znak. Klamačů je v nomenklátoru vypsáno sedm, avšak v praxi užíval šifrant i znaky bez významu, které v šifrovacím klíči ani uvedeny nejsou. Tak je tomu kupříkladu v dopisu z 30. prosince 1644,[115] kdy jsou některé klamače dokonce zvoleny tak, aby budily dojem kódu. Skutečných kódů je v šifrovacím klíči 31. Jim přiřazené šifrové znaky v posloupnosti navazují na bigramy,[116] avšak v konečném uspořádání je porušena pravidelnost. Kódy jsou uvedeny v němčině, ale nomenklátor lze použít i pro jiné jazyky, protože kódy pak byly jednoduše přeloženy do jazyka, v němž byla zpráva šifrována. To je vidět například na kopii italsky psaného dopisu z 2. prosince 1643, jehož odesílatelem byl markýz de Torrdelaguna.[117] Kromě dopisů v němčině a italštině jsou dochovány i příklady, kdy bylo této šifry užito ve španělském a latinském textu.[118]

Na příkladu německého slova *allen* si ukažme, jaké jsou možnosti obou šifer. Protože ve staré šifře může být každé písmeno nahrazeno dvěma různými šifrovými znaky, počet způsobů, jak zašifrovat slovo *allen*, je přesně 2^5, tedy 32.[119] S pomocí nové šifry je možné toto slovo zašifrovat 264 způsoby, nepočítáme-li s klamači.[120] Zahrneme-li i v nomenklátoru uvedené klamače, pak už je počet způsobů, při použití každého z nich maximálně jednou, větší než jedna miliarda. Nová šifra je tedy oproti té původní mnohem odolnější vůči frekvenční analýze. Samozřejmě ji i tak lze prolomit, ale trvalo by to mnohem delší dobu, než v případě staré šifry, jejíž slabinou je i systematické uspořádání šifrových znaků, kdy je možné šifrový klíč po odhalení několika šifrových znaků domyslet.

Bezpečnost šifry vůči náhodnému luštiteli do určité míry ovlivňovali i šifranti, jak dokládá psaní Ferdinanda III. z 25. září 1636,[121] utajené starou šifrou. Šifrant v tomto dopise přímo nad šifrové znaky doplňoval přehlásky. Tím práci případnému luštiteli ulehčil, protože prakticky označil samohlásky.

Pro představu, jaký typ zprávy mohl být předmětem utajení, poslouží Ferdinandův dopis z 26. července roku 1644,[122] který obdržel Matyáš Gallas během tažení císařské armády do Holštýnska. Císař v něm svému generál poručíkovi sděluje, že ho požádal Don Francisco de Melo prostřednictvím hraběte de Sa-

[115] Tamtéž, sign. XV/13, kart. 385.

[116] Bigramům odpovídají šifrové znaky 90-209, kódům pak šifrové znaky 210-240.

[117] HS Clam-Gallasů, sign. XV/3, kart. 375. Uvedený dopis leží ve válečné kanceláři samostatně, ale zdá se pravděpodobné, že byl přílohou dopisu, který snad Gallasovi zaslal Ferdinand III.

[118] Např. dopisy, označené v soupisu písemností čísly 63 a 108.

[119] V tabulce A.2.3 přílohy A.2 jsou vypsány všechny možnosti. Příslušné šifrové znaky jednotlivých písmen viz tabulka A.2.4.

[120] Všech 264 variant je vypsáno v tabulce A.2.1 přílohy A.2. Příslušné šifrové znaky jednotlivých písmen viz tabulka A.2.2.

[121] HS Clam-Gallasů, sign. XVIII/9, kart. 351.

[122] Tamtéž, sign. XV/9, kart. 381.

int Amour, aby poskytl vojsku španělského krále posilu, která by byla poslána k vojenskému ležení v Gravelines nebo v Lucembursku. Císař sice odvětil, že jeho armáda musí operovat proti nepříteli v Říši, avšak byl znovu požádán o čtyři regimenty, které nedávno dorazily z vévodství Jülich do Franků. Císař vysvětluje obavu, že by kvůli nedostatku vojska mohlo být Nizozemí ztraceno ve prospěch Francie, což je v konečném důsledku nebezpečím pro Říši i celý arcidům. Proto se rozhodl uvolnit požadované pluky. Dále píše podrobnosti k vykonání příkazu. K dopisu jsou přiloženy tři přílohy. Dvě z nich jsou rovněž šifrované. První šifrovanou přílohou je opis memoriálu hraběte de Saint Amour císaři, v němž zdůvodňuje potřebu pomoci pro španělského krále a navrhuje, aby pro ten účel císař uvolnil část Gallasových vojsk. Požadovaná posila by se měla skládat ze šesti nebo sedmi tisíc mužů. Druhá šifrovaná příloha je opis dopisu španělského krále Filipa IV. císaři, v němž referuje o dohodě Francie s Holandskem a žádá o pomoc. Mimo jiné apeluje na své příbuzenství a přátelství s císařem a jejich společné zájmy.[123]

Aby však bylo možné z obsahu šifrovaných dopisů vyvodit závěry, bude třeba prostudovat i další Ferdinandovy šifrované zprávy.

4.2.2 Šifra Matyáše Gallase s Ferdinandem von Bayern

Roku 1635 obdržel Matyáš Gallas tři šifrované písemnosti od kolínského arcibiskupa a kurfiřta Ferdinanda, bavorského vévody z rodu Wittelsbachů, jehož působení v době třicetileté války bylo úzce navázáno na politiku jeho bratra, kurfiřta Maximilána I.[124] Všechny tři dopisy jsou utajeny podle stejného šifrovacího klíče, který se do dnešních dnů nedochoval. U dopisu, který Ferdinand poslal Gallasovi 25. srpna,[125] je ale na samostatném listu přiložen dešifrovaný text. Díky jeho porovnání se šifrovým textem bylo možné příslušný klíč získat (viz tabulka 4.2.2).

Jedná se o jednoduchou substituci, obsahující šifrové znaky v podobě čísel a symbolů.[126] Pro šifrování zdvojeného písmene se využívalo dvou způsobů. Buď se použil dvakrát stejný znak, nebo byla šifrovému znaku příslušného písmene přidána vodorovná linie (např. CC=$\overline{\text{ɵ}}$,LL = $\overline{\triangle}$ či MM = $\overline{\text{♀}}$).

Z hlediska bezpečnosti lze šifru považovat za slabou už vzhledem ke svému typu. Je samozřejmě pravda, že v úvahách, zda by šifra splnila svou funkci před

[123] Obě přílohy jsou šifrované stejně jako vlastní Ferdinandův dopis, tj. novou šifrou mezi císařem a Gallasem. Otázkou je, zda byla tato šifra užita i v originálech příloh, pokud byly rovněž šifrovány. Jako pravděpodobnější se jeví vysvětlení, že císař nechal oba opisy pro Gallase přešifrovat, než že by v korespondenci se španělským králem užíval stejnou šifru jako s generálem.

[124] FRANZEN, August. *Ferdinand.* In: Neue Deutsche Biographie 5, 1961, s. 90 [online]. [cit. 7. 8. 2017]. Dostupné z: `https://www.deutsche-biographie.de/sfz56892.html#ndbcontent`.

[125] HS Clam-Gallasů, sign. XVIII/7, kart. 349.

[126] Šifrové znaky pro písmena *X*, případně *Y*, dosud odhaleny nejsou. Ve zkoumaných textech použity nebyly.

A	=	5	I	=	7	Q	=	◊
B	=	9̂	K	=	9̄	R	=	cr
C	=	ɵ	L	=	△	S	=	♁
D	=	1	M	=	♀	T	=	ω
E	=	6	N	=	0	V	=	9
F	=	2	O	=	8	W	=	n
G	=	3	P	=	+	Z	=	ô
H	=	4						

Tabulka 4.2.2: *Rekonstruovaný šifrovací klíč kurfiřta Ferdinanda*

náhodným luštitelem, je třeba zohlednit i další aspekty, například délku šifrového textu či práci šifranta, jak bylo ukázáno na jedné z šifer Matyáše Gallase s císařem. A právě dopis kurfiřta Ferdinanda z 25. srpna je dalším příkladem toho, jak mohl šifrant přispět k nežádoucímu odhalení utajeného obsahu. Chyba šifranta je uvedena v následujícím úryvku ze šifrového textu:

1 6 0 ♀ 6 △ 9̄ 6 *0* 5 *0* *0* 8 **1 6 3 0.** 6 7 0 3 6 4 5
N A N N O

Ve vlastním textu tajného sdělení je odkazováno na rok 1630, který šifrant nerozepsal slovně, ale ponechal v číselném tvaru. Aby naznačil, že se v tomto případě nejedná o šifrové znaky, umístil za číselný údaj tečku, čímž se toto místo v jinak bezprostředně po sobě jdoucích šifrových znacích stalo nápadné. Po odhalení významu znaků *1*, *6*, *3*, *0* lze tipovat, že se jedná o spojení *v roce 1630*, v německy psaném textu tedy *im Jahre* nebo tehdy běžně užívané latinské *anno*. A právě tady se šifrant dopustil dalšího nedopatření, když nevyužil šifrového znaku pro zdvojené N, ale použil příslušný šifrový znak dvakrát po sobě. Z toho lze tedy předpokládat, že 0 = N, čímž je shodou okolností prozrazeno druhé nejčastěji se vyskytující písmeno v německých textech,[127] a 8 = O. Protože předchozí slovo končí také na písmeno N, je rovněž jisté, že 5 = A. V případě luštění by pak byla první tři známá písmena dosazena na odpovídající místa v šifrátu a s jejich pomocí tak postupně rozklíčována další písmena.[128]

Pomocí získaného klíče je možné dešifrovat i zbylé dva dopisy, které dosud leží ve válečné kanceláři pouze ve své šifrované podobě. Zatím jsem takto dešifrovala psaní z 25. června.[129] Jde o supliku, která byla původně zaslána kurfiřtu Ferdinandovi z města Arnsbergu. Radní sdělují Ferdinandovi, že se generál Melander[130]

[127] Srov. KAŠPAR, J. *Příspěvek k řešení tajného písma*, s. 100.
[128] K postupu luštění monoalfabetických šifer srov. tamtéž, s. 95-107.
[129] HS Clam-Gallasů, sign. XVIII/6, kart. 348.
Viz obr. A.3.1 přílohy A.3.
[130] Peter Melander, vlastním jménem Peter Eppelmann hrabě von Holzappel. V době vzniku dopisu bojoval jako generál poručík lankraběte Viléma Hesensko-Kasselského proti císařským. Roku 1642 stranu změnil a stal se císařským polním maršálem. Srov. GEISTHARDT, Fritz.

vypravil 23. srpna s několika regimenty a děly k útoku na město Menden. Tuto noc, tedy z 24. na 25. června, se utábořil u měst Asseln, Brackel a [Wikhe].[131] Místo plánovaného útoku na Menden se ale cílem má stát právě Arnsberg, jak prý byli radní zpraveni od důvěryhodného posla. Navíc se má Melander spojit u [Frandenbergu][132] s plukovníkem [Crazensteinem], se kterým chtějí po obsazení Arnsbergu dobýt celý Sauerland.[133] Radní proto prosí kurfiřta, aby městu poslal vojenskou posilu. V dodatku z následujícího dne, 26. června, ale radní upřesňují, že nepřítel nakonec záměr změnil a s jedenácti pěšími a sedmi jízdními kompaniemi oblehl město Menden, které ostřeloval třemi malými dvoulibrovými děly. Napadl také města Medebach a Winterberg, vyplenil Hallenberg a proslýchá se, že se chystá drancovat i v sousedních městech, Schmallenbergu a [Fredeburgu].[134] Na závěr zástupci města Arnsbergu znovu prosí kurfiřta o včasné poslání posily.

Samotný dopis je vyjma oslovení a první věty šifrovaný kompletně, podobně v dodatku, kde je nešifrována pouze úvodní věta a datace. Obě písemnosti jsou nalepené na listu papíru, takže nejsou k dispozici případné poznámky na reversní straně. Dá se však předpokládat, že se dopis dostal do válečné kanceláře jako příloha dopisu, který Gallasovi zaslal kurfiřt Ferdinand.

4.2.3 Šifra Matyáše Gallase a Ottavia Piccolominiho

Ottavio Piccolomini, původem z toskánského šlechtického rodu, působil během třicetileté války jako vojevůdce na straně Svaté říše římské. Nejprve jako plukovník a kapitán Valdštejnovy tělesné stráže, od sklonku roku 1632 v hodnosti generál strážmistra a od podzimu následujícího roku coby generál jezdectva.[135] Během krize, vyvolané neshodami Valdštejna s císařem, zůstal věrný habsburskému arcidomu. Společně s Matyášem Gallasem a Janem Aldringenem se výrazně podílel na Valdštejnově pádu,[136] za což byl odměněn hodností polního maršála a mimo jiné panstvím Náchod. V květnu roku 1648 byl povýšen na generál poručíka.[137]

Ze vzájemné korespondence obou vojevůdců se ve válečné kanceláři dochovaly tři šifrované dopisy, u nichž víme s jistotou, že je odeslal Piccolomini Gallasovi.

Holzappel, Peter Graf zu. In: Neue Deutsche Biographie 9, 1972, s. 571 [online]. [cit. 8. 8. 2017]. Dostupné z: `https://www.deutsche-biographie.de/sfz33603.html#ndbcontent`.

[131] Asseln a Brackel jsou dnes části města Dortmund. Wikhe se mi dohledat nepodařilo.

[132] Vzhledem k poloze Dortmundu a města Menden by se mohlo jednat o dnešní město Fröndenberg/Ruhr.

[133] Vestfálský region, do něhož spadají právě města Menden či Arnsberg.

[134] Jedná se patrně o Bad Fredeburg, dnešní součást Schmallenbergu.

[135] BIERTHER, Kathrin. *Piccolomini, Ottavio Fürst.* In: Neue Deutsche Biographie 20, 2001, s. 408-410 [online]. [cit. 5. 8. 2017]. Dostupné z: `https://www.deutsche-biographie.de/sfz95776.html#ndbcontent`.

[136] REBITSCH, R. *Matyáš Gallas, s. 68.*

[137] BIERTHER, K. *Piccolomini*, s. 408-410.

První z nich je datován 20. července roku 1636,[138] druhý byl poslán v říjnu stejného roku.[139] Poslední z dopisů, a sice z 28. ledna 1643, je sám o sobě nešifrovaný, ale obsahuje krátkou šifrovanou přílohu.[140] Všechny tři dopisy jsou psány v italském jazyce.

Pro komunikaci Gallase s Piccolominim prostřednictvím tajných zpráv zůstaly ve válečné kanceláři dochovány dva šifrovací klíče označené jako:

Alte Piccolominische Zieffer (viz tabulka 4.2.3)
Newe Zieffer mit h[errn] Graufen Piccolomini[141] (viz tabulka 4.2.4)

V obou případech se jedná o homofonní substituci. Ve staré šifře je ovšem homofonie využita pouze u samohlásek a písmene F. To je ale u šifrovacího klíče zamýšleného pro italský text jako opatření proti frekvenční analýze nedostatečné, protože jedním z charakteristických rysů italštiny je zdvojení souhlásek.[142] V nové šifře je tato slabina částečně odstraněna tím, že jsou většině písmen přiřazeny dva šifrové znaky. Toto malé posílení bezpečnosti šifry bude ale spíše důsledkem sestavení klíče, než záměrem. Oproti staré šifře, v níž jsou šifrové znaky písmenům přiřazeny náhodně, je totiž nová šifra vytvořena na základě systému, z něhož je patrné, proč má sedm písmen pouze jeden šifrový znak.

Oba dopisy z roku 1636 jsou utajené pomocí staré šifry. Šifrované sdělení v příloze zprávy z roku 1643 ovšem neodpovídá ani jedné z obou uvedených šifer. Nelze na něj použít žádný jiný dochovaný šifrovací klíč a k dispozici není ani dešifrovaný text. Jisté je, že se jedná o typ substituční šifry. Od staré i nové šifry se ale tato liší podobou šifrových znaků. Jsou jimi písmena v kombinaci s jednociferným až trojciferným číslicemi. Šifrové znaky v podobě dvojciferných a trojciferných čísel jsou navíc označeny buď křížkem, nebo kolečkem. S velkou pravděpodobností tak půjde rovněž o homofonní substituci, popřípadě dokonce nomenklátor.

Vedle tří uvedených písemností se k Piccolominimu váže ještě jeden soubor dopisů, který leží v registratuře pod datem 21. března 1643.[143] Jde o originál německy psaného dopisu saského kurfiřta Jana Jiřího I., adresovaného Piccolominimu, k němuž je přiloženo několik kopií různých dopisů. Jedna z těchto kopií je

[138] HS Clam-Gallasů, sign. XVIII/8, kart. 350.
[139] Tamtéž, sign. XVIII/9, kart. 351.
[140] Tamtéž, sign. XVIII/23, kart. 365.
[141] Tamtéž, sign. XV/20, kart. 392.
[142] Někteří tvůrci šifrovacích klíčů si toho byli vědomi, jak vyplývá z jiného, blíže neurčeného, šifrovacího klíče z Gallasovy registratury. Jde o nomenklátor, vytvořený pro italský text, kde je homofonní substituce doplněna speciální poznámkou o způsobu šifrování zdvojených písmen. Srov. tamtéž.
[143] Tamtéž, sign. XVIII/23, kart. 365.

A	=	99, 26, 18	I	=	83, 38, 29	R	=	98
B	=	30	K	=	14	S	=	23
C	=	47	L	=	76	T	=	44
D	=	10	M	=	54	V	=	97, 81, 39
E	=	15, 68, 21	N	=	12	W	=	50
F	=	57, 63, 95	O	=	35, 77, 19	X	=	90
G	=	17	P	=	55	Y	=	60
H	=	28	Q	=	66	Z	=	84

Tabulka 4.2.3: *Stará šifra s Piccolominim*

A	=	16, 61	I	=	32, 23	R	=	48, 84
B	=	18, 81	K	=	34, 43	S	=	50
C	=	20	L	=	36, 63	T	=	52, 25
D	=	22	M	=	38, 83	V	=	54, 45
E	=	24, 42	N	=	40	W	=	56, 65
F	=	26, 62	O	=	42, 24	X	=	58, 85
G	=	28, 82	P	=	44	Y	=	60
H	=	30	Q	=	46, 64	Z	=	62, 26

Tabulka 4.2.4: *Nová šifra s Piccolominim*

šifrována. Kromě data v ní chybí i jméno odesílatele a příjemce. Vzhledem k oslovení „Hochwolgebohrner herr General vndt VeldtMarshalek, Gnediger herr“ by snad adresátem mohl být právě Piccolomini, což však může objasnit jen detailnější prostudování obsahu celého tohoto souboru dopisů. Zatím lze jistě tvrdit jen to, že použitá šifra neodpovídá ani jedné ze tří šifer mezi Piccolominim a Gallasem. Text není dešifrován a utajené části sdělení jsou příliš krátké, takže je nelze luštit na základě frekvenční analýzy. S výjimkou osmi šifrových znaků jsou totiž všechny ostatní v šifrátu zastoupeny právě jednou. Opět ale nejspíše půjde o homofonní substituci.

Pomineme-li poslední zde uvedený šifrovaný dopis, u něhož není jisté, jestli vůbec bylo zamýšleno, aby ho Gallas četl, víme, že oba vojevůdci ve vzájemné korespondenci používali minimálně tři šifry. Z druhé poloviny roku 1636 máme doklady o užívání staré šifry. Z kraje roku 1643 pak bylo k výměně tajné zprávy použito šifrovacího klíče, který není dochován. Z válečné kanceláře Matyáše Gallase tak není možné zjistit, v kterých letech byla v užívání šifra označená jako *nová*. Zdá se ale pravděpodobné, že to bylo ještě během Gallasova prvního generalátu, vzhledem k tomu, že jsou oba dochované šifrovací klíče zaznamenány jednou písařskou rukou na jednom listu. Přesnější odpověď se ale možná skrývá v *Rodinném archivu Piccolominiů*, uloženém v SOA v Zámrsku, kde by měly být dochovány písemnosti, které adresoval Piccolominimu Gallas.

4.2.4 Šifra Waltera Leslieho

K datu 12. července 1644 je ve válečné kanceláři uložen italsky psaný šifrovaný dopis, pod nímž je podepsán Walter Leslie,[144] voják skotského původu, který vstoupil do císařské armády roku 1631. Svoji vojenskou dráhu zde začal jako plukovník-strážmistr v pěším pluku generála Adama Erdmanna Trčky. Jeho zásadní role v chebských únorových událostech roku 1634 mu vynesla zásluhy v podobě jmenování do hodnosti plukovníka pěšího regimentu, úřad komorníka a panství Nové Město nad Metují, které do té doby patřilo Trčkům z Lípy. O tři roky později byl povýšen do stavu říšských hrabat. Jeho kariéra rostla i po skončení třicetileté války, kdy byl povýšen na polního maršála a stal se viceprezidentem dvorské rady válečné. Později se uplatnil i v diplomatických službách.[145]

Není známo, komu byl dopis adresován. Mezi řádky je vepsán dešifrovaný text, což vytváří dojem, že Gallas musel vlastnit klíč, a tedy že byl dopis určen pro něj. On sám příjemcem ale určitě nebyl, protože se o něm v dopisu mluví ve 3. osobě. Psaní bylo nejspíš dešifrováno ještě předtím, než se dostalo do jeho válečné kanceláře.

Z klíče, který bylo možné částečně sestavit díky přepisu šifrátu do otevřeného textu, je vidět, že jde o nomenklátor, vytvořený z homofonní šifrové abecedy a kódů (viz tabulka 4.2.5). Může obsahovat i trigramy či bigramy. V šifrovém textu se totiž objevily tři šifrové znaky, u nichž nelze s jistotou určit, zda se v šifrovacím klíči nacházely mezi kódy nebo mezi trigramy. Jedná se konkrétně o šifrové znaky pro **che**, **con** a **tra**, na které lze nahlížet jako na samostatná slova, tedy zájmeno **který** a předložky **s** a **mezi**, nebo na součást jiných slov (např. perché, recondito, nostra). Zmíněné šifrové znaky jsou v dopisu použity v obou jmenovaných případech.

Nad některými šifrovými znaky jsou připsány samohlásky *a*, *e* nebo *o*. Označení *e* znamená, že se jedná o zdvojené písmeno. Symbol *a* se v šifrovém textu vyskytl pouze jednou, kdy 30^a bylo dešifrováno jako 30 000. Vypadá to tedy, že znak *a* byl využíván v souvislosti se značením čísel, avšak nemůžeme na základě jednoho příkladu zobecnit, jakou přesně měl funkci. Podobně je tomu i u znaku *o*. Šifrové znaky takto označené byly při dešifrování ve všech případech přeskočeny. To napovídá, že by mohlo jít o bludičky. Je to však pouze hypotéza, k jejímuž ověření bychom museli mít k dispozici více šifrovaných dopisů Waltera Leslieho.

[144] HS Clam-Gallasů, sign. XV/9, kart. 381.
Ukázka z dopisu viz obr. A.3.2 přílohy A.3.

[145] BROUCEK, Peter. *Leslie, Walter von.* In: Neue Deutsche Biographie 14, 1985, s. 331 f. [online]. [cit. 6. 8. 2017]. Dostupné z: `https://www.deutsche-biographie.de/gnd122181220.html#ndbcontent`.

Klíč pro homofonní substituci:

A	=	16, 17	H	=	24	Q	=	41
B	=	10	I	=	36, 37	R	=	44
C	=	11	L	=	31	S	=	52, 53
D	=	14	M	=	34	T	=	60
E	=	26, 27	N	=	42	U,V[146]	=	56, 57
F	=	20	O	=	46, 47	W	=	šifruje se jako VV
G	=	21	P	=	40			

Kódy:
48 = S. M. Ces^a (S[acra] M[ajestas] C[a]es[area])
65 = V. E. (V[ostra] E[ccellenza] (?))

Kódy či trigramy:
18 = con
22 = che
35 = tra

Další znaky:
30^a = číslo 30 000

Tabulka 4.2.5: *Rekonstruovaná část šifrovacího klíče W. Leslieho*

Transliterace šifrované a dešifrované části dopisu:

S výjimkou několika úvodních a závěrečných řádků je celý dopis šifrován, aniž by byl prokládán nešifrovanými částmi. Vlivem drobných chyb v podobě „překlepů“ v šifrových znacích, zapomenutých šifrových znaků, vypadlých písmen či zkracování slov není dešifrovaný text úplně shodný se šifrátem. V přepisu, který následuje, je uvedena zašifrovaná část dopisu. Členění textu je ponecháno shodně s předlohou. Primárně je text transliterován podle toho, jak je zašifrován. Pokud se dešifrovaný text liší, je příslušný rozdíl uveden v hranaté závorce.

1. strana:
Nelle presenti *congiunture* [congionture]
S. M. Ces^a non *pol mandar* [può mandare]
un huomo di soccorso
V. E. sa che il Galasso non permettera
mai di *leuar* [leuare] un huomo
della [dlla] sua Armata
le cose in *Hunharia*[147] [Vngaria] Vanno

[146] V dešifrovaném textu, který je psán humanistickým písmem, je rozlišováno mezi písmeny *U* a *V*. V šifrovém textu oběma písmenům odpovídají shodné šifrové znaky.
[147] Mezi šifrovými znaky pro písmena *N* a *H* je vložen šifrový znak 34^o.

[molto][148] mole per mancamento
di Gente e la nostra Armata
Si *retira* [ritira] à
bon [buon] passo, e lo nemico la
seguita Questo *pol* [puol]
disturbare e disconcertare

2. strana:
tutte *le opperationi* [l'operationi]
del *Gallaoso* [Galasso]
co [con] più di 30 000 Turchi sopra le frontiere
e sin hora
non siamo sicuri
di loro per questo
V. E. non ha da far fondamento
di *hauer* [hauere] un huomo
di quà e *si* [se] V. E. *uol* [uuol]
hauerà *giente* [gente] da S. M. Ces^a fra tre
o *quauro* [quattro] mesi o per
l'anno che uiene *bisgna* [bisogna]
dar [dare] il danaro adesso
per far leuate. In *VVastfallia* [Wesfaglia]
V. E. *fa* molto bene non *di*[149]
accettar *nisun* [nissun] comando
in *qesti* [questi] (?)[150] *catiui* [cattiui] tempi
uoless [volesse] dio che
il *Parlameto* [Parlamento] de Ingelterra [di Inghilterra]
hauesse *arestato* [arrestato]
la persona di V.E. per questo

3. strana:
estade [estate] perche ho paura che
V.E. perdera assai di esser
andato con *Don* [D.] Francesco
in Campagna V.E. hà fatto
molto bene per il

[148] V šifrovém textu chybí.
[149] Slova „fa" a „di" v dešifrovaném textu chybí.
[150] V šifrovém textu se na tomto místě nachází šifrové znaky 57^o a 36^o.

seruisio[151] del Re ma
molto male per se [se][152] stesso

4.2.5 Šifra Matyáše Gallase s markýzem di Grana a hrabětem Kurtzem

Z let 1637 a 1643 máme dochováno dohromady deset šifrovaných dopisů, jejichž odesílatelem byl Francesco Caretto, markýz di Grana, císařský polní zbrojmistr a později vyslanec u dvora španělského krále.[153] Všechny zprávy jsou psány německy a jsou utajeny podle stejného klíče. Ten se nedochoval, ale z přepisů některých dopisů do otevřeného textu jej bylo možné částečně sestavit (viz tabulka 4.2.6). Gallas s markýzem di Grana si šifrovali zprávy pomocí nomenklátoru, který se skládá z homofonní substituce, klamačů a většího množství kódů. Právě existence nemalého počtu kódů je důvodem, proč nebylo možné, rekonstruovat klíč úplně. Aby byl ale výsledek co nejpřesnější, využila jsem všech šesti dopisů, u kterých zůstal dochován dešifrovaný text.

V homofonní šifře jsou jednotlivým písmenům abecedy přiřazeny dva šifrové znaky – jeden je vždy dvojciferné číslo, ležící v intervalu mezi čísly 13 a 48, a druhý pak písmeno, případně symbol.[154] Klamačů se mi podařilo s jistotou identifikovat 16. Jsou jimi právě ta dvojciferná čísla, která nejsou v uvedeném intervalu obsazená jako šifrové znaky pro písmena abecedy, včetně tří dalších šifrových znaků vně intervalu. Ve dvou dalších případech jsem narazila na šifrové znaky, kterým nebylo možné přiřadit znak otevřeného textu, ale zároveň je nešlo na základě jednoho výskytu automaticky zařadit mezi bludičky. Vzhledem k množství překlepů, kterých se dopouštěl markýzův šifrant, totiž nelze vyloučit, že byly použity omylem a v šifrovacím klíči se ve skutečnosti nevyskytovaly. Kódům odpovídající šifrové znaky jsou trojciferná čísla, uspořádána vzestupně. Jednotlivá slova jsou jim přiřazena abecedně, ačkoli alfabetické řazení ve skupinách slov se shodným počátečním písmenem není důsledně dodržováno (např. 191 = Erfurth, 192 = Engelandt). Z dostupného šifrového materiálu jsem byla schopna určit 42 kódů, ale nanejvýš pravděpodobně se nejedná o závěrečný počet. Pokud byly zastoupeny všechny číslice mezi prvním a posledním kódem ve výše uvedeném seznamu, pak jich tento nomenklátor obsahoval minimálně 231. Na základě odhalených kódů je zřejmé, že se jimi obsazovaly geografické názvy, tituly, slova z vojenského okruhu

[151] Mezi šifrovými znaky pro písmena E a R je vložen šifrový znak 57^o.
[152] V dešifrovaném textu je uvedené dvakrát.
[153] REBITSCH, R. *Matyáš Gallas*, s. 102, 197.
[154] Pro písmeno X jsem ve vzorku zkoumaných textů našla pouze jeden šifrový znak. Předpokládám však, že je to způsobeno obecně nízkým výskytem tohoto písmene v německých textech, a že tedy ve skutečnosti druhý šifrový znak existoval. Podobně je tomu s písmenem Q, které jsem našla jedenkrát až v blíže neurčeném italsky psaném konceptu. Viz níže.

Klíč pro homofonní substituci:

A	=	13, b	I	=	29, n	R	=	41, w
B	=	15, d	K	=	31, o	S	=	42, x
C	=	17, f	L	=	33, p	T	=	43, Z
D	=	19, g	M	=	35, q	V	=	44, a
E	=	21, h	N	=	37, r	W	=	45, c
F	=	23, K	O	=	38, 5	X	=	46
G	=	25, L	P	=	39, 4	Y	=	47, ⟠
H	=	27, m	Q	=	40	Z	=	48, y

Klamače:
9, 10, 11, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36

Nejasné šifrové znaky:
3, 8

Kódy (ponechány v dobovém pravopisu):

134	=	Armada	258	=	Landgraff
142	=	Abgesandten	267	=	Marggraff
160	=	Chur Sachßen	270	=	Musterplätz
161	=	Chur Brandeburg	287	=	Niederlandt
176	=	Dennemarkht	290	=	Obrister
191	=	Erfurth	294	=	protestirende
192	=	Engelant	296	=	Pfalczgraff
200	=	Fürsten	307	=	Römisches Reich
205	=	feindt	310	=	regiment
206	=	Frankreich	311	=	Ritmeister
207	=	friedt	313	=	[Rheinstrom]
218	=	Graf	315	=	Rath
219	=	gelt	321	=	Soldat
227	=	Herzog	332	=	Spanien
228	=	Hessen	334	=	Teutschlandt
232	=	herr	335	=	Teutschmeister
233	=	hilf	336	=	Türkhen,Türkhey
241	=	(Ihr) Kaiserliche Majestät	344	=	Volkh
242	=	Königliche Majestät	345	=	und
252	=	krieg	346	=	von
257	=	Landt	364	=	zu(e)

Tabulka 4.2.6: *Rekonstruovaná část Carettova šifrovacího klíče*

i často užívané spojky a předložky. Podle způsobu šifrování prostudovaných šifrovaných dopisů Francesca Caretta to vypadá, že naopak seznam kódů neobsahoval jména konkrétních osob.

Shodnou šifru jsem kromě dopisů markýze di Grana objevila ve čtyřech dalších případech z roku 1638. Dva z nich potvrzují, že Matyáš Gallas užíval to-

hoto nomenklátoru také v korespondenci s říšským vicekancléřem Ferdinandem Zikmundem hrabětem Kurtzem von Senftenau.[155] První písemností je koncept dopisu z července uvedeného roku,[156] u něhož jsou zachovány krátké šifrované pasáže a který na reversní straně nese jméno právě hraběte Kurtze. Zpráva, která Gallasovi dorazila 25. srpna 1638,[157] je jako jedna z mála šifrována kompletně bez jediného znaku otevřeného textu, avšak jméno odesílatele je zaznamenáno na reversní straně písemnosti, takže bylo opět možné identifikovat hraběte Kurtze. Dopis přináší informace z rezoluce dánského krále.

Ve zbylých dvou případech,[158] kde je tato šifra užita, a sice výtah z dopisu z 18. července 1638 a koncept dopisu z 8. srpna téhož roku, není možné rozhodnout, kdo byl jejich odesílatelem. U posledně jmenovaného je zajímavé, že je psán na rozdíl od všech dosud zmíněných dopisů italsky, čímž se ukazuje, že při vzniku nomenklátoru nebylo zamýšleno jeho užívání výhradně pro jeden jazyk.

4.2.6 Zachycené šifrované dopisy na příkladu zpráv Lennarta Torstenssona

V předchozích ukázkách jsme se snažili nahlédnout na zkoumané šifry i z pozice náhodného luštitele. Tento pohled má své opodstatnění, protože zašifrování obsahu dopisu mělo být obranou právě před případným nežádoucím čtením. Utajování obsahu zpráv také naznačuje, že si korespondenti uvědomovali, že při výměně dopisů dochází k jejich odchytávání nepřátelskou stranou. To nám nakonec dosvědčuje i válečná kancelář, kde je uloženo několik šifrovaných[159] dopisů, které jsou na reversní straně explicitně označeny jako *Intercipirtes Schreiben*, tedy *zachycené psaní*. Z těchto zachycených dopisů se blíže podíváme na dva z nich, a to na dopisy švédského generála Lennarta Torstenssona, který stanul v čele švédské armády po smrti polního maršála Jana Banéra[160] roku 1641. V polním maršálovi Torstenssonovi, který byl vynikajícím vojevůdcem, stratégem a dělostřeleckým

[155] Říšským vicekancléřem se hrabě Kurtz stal koncem roku 1637. Mimo jiné působil také jako říšský dvorní rada, později se stal členem tajné rady. Uplatnil se i na poli diplomatickém. Do stavu říšských hrabat byl povýšen roku 1636. Srov. RIEDENAUER, Erwin. *Kurtz von Senftenau, Ferdinand Sigismund Graf*. In: Neue Deutsche Biographie 13, 1982, s. 328 f. [online]. [cit. 9. 8. 2017]. Dostupné z: `https://www.deutsche-biographie.de/sfz47164.html#ndbcontent`.

[156] HS Clam-Gallasů, sign. XVIII/18, kart. 360.

[157] Tamtéž.

[158] Tamtéž.

[159] To samozřejmě nevylučuje, že se v Gallasově registratuře nachází i zachycené dopisy nešifrované. Ty však nebyly blíže zkoumány, neboť nejsou předmětem této práce.

[160] Coby vojevůdce třicetileté války je Jan Banér hodnocen jako jeden z nejlepších. Nebál se riskovat, vyznačoval se mimo jiné rychlými pochody, včetně zimních tažení, která u něj obdivoval i císař Ferdinand III., byť jejich následkem umírali i Banérovi vojáci. Ve vojenských akcích se Banér projevoval agresivně, na rozdíl od Gallase, pro něhož je charakteristický defenzivní způsob vedení války. Srov. REBITSCH, R. *Matyáš Gallas*, s. 111, 146.

specialistou, „získal“ Matyáš Gallas dalšího velkého protivníka.[161]

Prvním z obou zachycených dopisů generála Torstenssona je psaní z 14. července 1644,[162] jehož adresátem byl švédský vyslanec, hrabě Johan Axelsson Oxenstierna.[163] Ačkoli mu měl dopis dorazit do Osnabrücku, skončil v Gallasově válečné kanceláři. Obsah dopisu je z převážné části šifrován, jen místy prokládán nešifrovanými pasážemi, z kterých je poznat, že se jedná o zprávu ve švédštině. Následný osud tohoto Torstenssonova utajeného sdělení je zaznamenán v nešifrovaném dopisu císaře Ferdinanda ze 7. září roku 1644.[164] Císař Gallasovi píše, že nechal rozluštit odchycené dopisy Torstenssona, určené švédskému vyslanci, tedy Oxenstiernovi, v Osnabrücku. Z přiložených opisů může prý Gallas vidět, jakými záludnými úmysly se nepřítel řídil a podle toho se teď generál poručík může zařídit. Kromě opisů rozluštěných zachycených zpráv přikládá císař i samotný šifrovací klíč, aby jej Gallas mohl použít v případě, že se mu do rukou dostanou další listy švédského generála. Příloha obsahuje dvě kopie rozluštěných zachycených dopisů. Jedna z nich odpovídá právě Torstenssonovu psaní ze 14. července. Na rozdíl od originálu je ale přeložena do němčiny. Zmiňovaný šifrovací klíč se v Gallasově válečné kanceláři bohužel nedochoval. Vzhledem k překladu nelze ani provést jeho rekonstrukci pomocí opisu. Luštění je zase podmíněno znalostí švédštiny. Je však možné, že je klíč stále dochován ve Švédsku v archivu, kde je dnes uložena Torstenssonova pozůstalost, respektive válečná kancelář. Vedle Švédska přichází v úvahu ještě možnost, že si klíč pro případnou další potřebu ponechal i císař. Na základě toho jsem se pokusila o jeho dohledání v oddělení Válečného archivu Rakouského státního archivu ve Vídni. Vytipovala jsem k tomuto účelu písemnosti fondu Stará polní akta (Alte Feldakten), které se týkají třicetileté války pro rok 1644. Příslušný klíč jsem však nenašla, což ovšem neznamená, že neexistuje v jiném fondu či oddělení Rakouského státního archivu.

O samotné šifře lze říci tolik, že se jedná o substituci. Šifrovými znaky jsou jednociferná až čtyřciferná čísla. Vzhledem k počtu šifrových znaků a výskytu čtyřciferných čísel bude klíčem pravděpodobně složitější nomenklátor.

Druhý dopis poslal Torstensson dne 26. srpna roku 1644[165] švédskému generál

[161] Tamtéž, s. 138.

[162] HS Clam-Gallasů, sign. XV/9, kart. 381.

[163] Syn švédského státníka, kancléře Axela Oxenstierny. Působil jako tajný rada krále Gustava II. Adolfa a později člen poručnické vlády královny Kristýny. Roku 1641 byl svým otcem vyslán do Německa, kde měl na mírových jednáních v Osnabrücku prosazovat otcovy politické zájmy na úkor přání královny Kristýny, žádající rychlé uzavření míru. Srov. životopisný portrét J. A. Oxenstierny na webovém portálu „Westfälische Geschichte“, který vznikl pod záštitou Institutu pro regionální dějiny Vestfálska. [cit. 11. 8. 2017]. Dostupné z: `http://www.lwl.org/westfaelische-geschichte/portal/Internet/finde/langDatensatz.php?urlID=5504&url_tabelle=tab_person`.

[164] HS Clam-Gallasů, sign. XV/11, kart. 383.

[165] Tamtéž, sign. XV/10, kart. 382.

Klíč pro homofonní substituci:

A	=	16, 100	H	=	2, 23, 88	R	=	27, 78
B	=	14, 20, 40	I	=	9, 44	S	=	5 (?), 102
C	=	17, 70	L	=	58	T	=	28, 95, 101
D	=	21	M	=	77	V	=	4
E	=	18, 57, 85	N	=	6, 91	W	=	1, 99
F	=	22	O	=	12, 68			

Bigramy a trigramy:
292 = di
294 = den
295 = da

Tabulka 4.2.7: *Rekonstruovaná část šifrovacího klíče „Torstensson–Königsmarck“*

majorovi Hansi Christophu Königsmarckovi.[166] Toto odchycené psaní je v Gallasově válečné kanceláři označeno jako duplikát. Dopis je šifrován částečně a je psán německy. Zachycený dopis pak Gallas zaslal císaři, což potvrdil sám Ferdinand III., když 24. září 1644 napsal Gallasovi, že obdržel jeho relaci ze 14. září s připojeným šifrovaným psaním Torstenssona Königsmarckovi. V této souvislosti je dále uvedeno, že byl k Torstenssonovu psaní nalezen klíč, který bude poslán Gallasovi pro případ dalších zachycených listů.[167] Klíč se opět nedochoval, ale u dopisu zůstala příloha, a sice dešifrovaný text Torstenssonova šifrovaného dopisu. Je tedy možné, klíč získat srovnáním obou písemností. Protože se však dešifrovaný text do určité míry liší od své šifrové podoby,[168] podařilo se mi zatím rekonstruovat pouze menší část klíče (viz tabulka 4.2.7).

Ze získané části šifrovacího klíče je vidět, že se jedná o nomenklátor, o němž prozatím víme, že obsahuje homofonní substituci a šifrové znaky pro bigramy a trigramy. Šifrovými znaky jsou jednociferná až trojciferná čísla. Za zajímavost stojí, že ani císař neměl k dispozici celý šifrovací klíč, protože v dešifrovaném textu zůstalo několik šifrových znaků nerozluštěných. I tak se ale císařské kanceláři

[166] Hans Christoph hrabě Königsmarck pocházel z města Kötzlin v Německu. Na bojiště třicetileté války vstoupil roku 1620 na straně císařských. Roku 1631 však nabídl své služby švédskému králi Gustavu II. Adolfovi a do konce války už bojoval ve švédských barvách. Roku 1640 byl povýšen na generál majora, o osm let později se stal polním podmaršálem. Roku 1648 dobyl Malou Stranu a zabavil rudolfinské sbírky, které byly následně odvezeny do Švédska. Mimo jiné byl za to povýšen do hraběcího stavu. Srov. SCHULZE, Heinz-Joachim. *Königsmarck, Hans Christoph Graf von.* In: Neue Deutsche Biographie 12, 1979, s. 360 f. [online]. [cit. 11. 8. 2017]. Dostupné z: `https://www.deutsche-biographie.de/sfz43859.html#ndbcontent`.

[167] HS Clam-Gallasů, sign. XV/11, kart. 383. Tento císařův dopis šifrovaný není.

[168] Odlišnosti dešifrovaného textu oproti šifrátu nejsou zvláštností tohoto příkladu. S touto skutečností jsem se setkala u všech dopisů, u nichž jsem rekonstruovala klíč. Jedná se o odlišnosti vzniklé neustáleností pravopisu německého jazyka té doby. Např. Feind X Feindt, gnädig X gnedig, apod. V dalších případech může jít o překlepy, jak bylo ukázáno na dopisu Waltera Leslieho.

podařilo rekonstruovat klíč do té míry, že bylo možné získat obsah šifrovaného sdělení.

Díky dochovaným listům císaře adresovaných v této záležitosti Matyáši Gallasovi máme představu, jakým způsobem asi postupoval generál poručík při zachycení dopisu nepřátelské strany. Na dvou konkrétních příkladech jsme rovněž poznali, jak bylo úspěšné jejich luštění v rámci císařské kanceláře. Ačkoli na základě dvou příkladů nelze zobecnit odpověď na otázku, jak účinné bylo šifrování dopisů v praxi, respektive s jakou úspěšností se dařilo luštit šifry v zachycených dopisech protivníka, přeci jen nám uvedené příklady odpověď alespoň poodhalují a umožňují částečně korigovat již vyslovené předpoklady a hypotézy. V této souvislosti připomeňme článek Jakuba Mírky o šifrované korespondenci v SOA v Plzni, který se také dotýká otázky zachytávání dopisů. V článku je k tomu jako jeden z příkladů uvedena zachycená kopie německy psaného dopisu z Gallasovy válečné kanceláře. Jde o psaní švédského královského rady Alexandra Erskina Johannu Adlerovi Salviovi[169] ze dne 15. července 1644.[170] Protože dopis leží v Gallasově registratuře bez vepsaného či přiloženého dešifrovaného textu, autor předpokládal, že šifra nejspíš prolomena nebyla a šifrování tak splnilo účel.[171] Je ale možné, že dopis ve skutečnosti rozluštěn byl a příslušný dešifrovaný text jen leží ve válečné kanceláři na jiném místě, stejně jako v případě dopisů Lennarta Torstenssona. Pokud by se Erskinův šifrovací klíč podobal ostatním šifrám, které jsme rozebírali v rámci válečné kanceláře, a pokud by se zachycený dopis dostal k vyluštění do kanceláře císařské, zdá se navíc dokonce pravděpodobné, že rozluštěn byl. Jsou to však zatím jen další hypotézy, které bude nutné ověřit hlubším zkoumáním nejen šifrované korespondence Gallasovy válečné kanceláře.

[169] Švédský tajný rada, dvorský kancléř a diplomat. Byl mimo jiné vyslancem na mírových jednáních v Osnabrücku, kde na rozdíl od J. A. Oxenstierny zastupoval zájmy královny Kristýny. Srov. životopisný portrét J. A. Salvia na webovém portálu „Westfälische Geschichte“. [cit. 12. 8. 2017]. Dostupné z: `http://www.lwl.org/westfaelische-geschichte/portal/Internet/finde/langDatensatz.php?urlID=5505&url_tabelle=tab_person`.

[170] HS Clam Gallasů, sign. XV/9, kart. 381.

[171] MÍRKA, J. *Raně novověká šifrovaná korespondence*, s. 68, 72.

Závěr

Šifrovaná korespondence jako součást válečné kanceláře Matyáše Gallase je v této práci nejprve popsána z hlediska jejího podílu vůči celkové písemné agendě generál poručíkovy vojenské registratury. Všechny šifrované písemnosti jsou zaznamenány v přiloženém soupisu s uvedením základních údajů. Na vybraném vzorku šifrovaných dopisů jsou ukázány typy šifer, jejich odolnost vůči náhodnému luštění či případné obměny šifrovacích klíčů. Nastíněna je rovněž praxe zachytávání dopisů nepřátelské strany a úspěšnost při pokusu o prolomení šifry v císařské kanceláři. Výběr zkoumaných dopisů časově pokrývá období obou Gallasových generalátů, na něž šifrovaná korespondence připadá, a z okruhu korespondentů představuje osoby z různého prostředí, byť je patrná převaha osob z prostředí vojenského.

Všechny zkoumané dopisy jsou šifrovány buď pomocí některé z variant substituční šifry, které využívají pouze jednu šifrovou abecedu, nebo pomocí nomenklátoru. V žádném ze zkoumaných textů nebyla použita transpoziční šifra, ba dokonce v žádné šifrované písemnosti válečné kanceláře vůbec, což je možné konstatovat s jistotou, neboť samotné rozpoznání transpozice či substituce umožňuje podoba šifrových znaků v šifrovém textu. Tento závěr koresponduje s výsledky bádání Jakuba Mírky, shrnutými v článku *Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni*, který rovněž nenalezl žádné šifrované písemnosti, v nichž by bylo využito transpozice.[172]

Šifrovými znaky v šifrovaných dopisech Gallasovy válečné kanceláře jsou převážně číslice, jen v některých málo případech i písmena či symboly. Tato skutečnost podporuje tvrzení, že v době raného novověku začaly číslice coby šifrové znaky převažovat, a to s ohledem na rostoucí užívání nomenklátoru, pro jehož sestavení bylo často potřeba většího počtu šifrových znaků.[173]

Tezi, že šifrovací klíče raně novověkého vojenského prostředí bývaly jednodušší,[174] lze podpořit, hodnotíme-li v praxi užívané šifry v konfrontaci s kryptologickými znalostmi doby.[175] V případě srovnávání šifrovacích klíčů vojenského okruhu s jinými sférami (např. diplomatické prostředí) je však nutné, posuzovat šifry v kontextu jednotlivých korespondentů a jejich společenského postavení. Jak

[172] MÍRKA, J. *Raně novověká šifrovaná korespondence*, s. 46.
[173] Tamtéž, s. 47.
[174] Tamtéž, s. 68.
[175] Teoretické znalosti z oblasti kryptologie byly v době Matyáše Gallase na vyšší úrovni, než na které jsou založeny šifry v písemnostech jeho válečné kanceláře. Např. polyalfabetická substituce byla známa již od doby Leona Battisty Albertiho (1404–1472). Srov. VONDRUŠKA, P. *Šifrování*, s. 213.

se totiž ukazuje po rozboru šifrovaných dokumentů válečné kanceláře, propracovanější nomenklátory mohou ležet i v registraturách vojevůdců třicetileté války, a to nejen těch, kteří bojovali na katolické straně, jak jsme poznali na příkladu zachycených dopisů švédského generála Torstenssona. Ovšem vzhledem ke skutečnosti, že detailnějšímu rozboru byl podroben jen výběr šifrovaných písemností, byly by nyní jednoznačné závěry předčasné.

Ve studiu šifrovaných písemností Gallasovy registratury je nutné dále pokračovat, aby bylo možné dílčí poznatky a hypotézy, které byly v této práci vysloveny, jasně potvrdit či vyvrátit. Rovněž je třeba zdůraznit, že rozbor šifrovaných písemností je zde veden převážně z hlediska paleografie a má sloužit jako podklad k dalšímu bádání. Pro získání uceleného obrazu o šifrované korespondenci válečné kanceláře bude nezbytné provést analýzu dopisů také z hlediska diplomatiky, čemuž bych ráda dále věnovala.

Seznam pramenů a literatury

Prameny nevydané

SOA v Litoměřicích – pobočka Děčín, Historická sbírka (rodinný archiv) Clam-Gallasů, Frýdlant, inv. č. 1397, sign. XVIII/5, kart. 347.

sign. XVIII/6, kart. 348.

sign. XVIII/7, kart. 349.

sign. XVIII/8, kart. 350.

sign. XVIII/9, kart. 351.

sign. XVIII/10, kart. 352.

sign. XVIII/11, kart. 353.

sign. XVIII/12, kart. 354.

sign. XVIII/18, kart. 360.

sign. XVIII/19, kart. 361.

sign. XVIII/20, kart. 362.

sign. XVIII/23, kart. 365.

sign. XVIII/27, kart. 369.

sign. XVIII/28, kart. 370.

sign. XVIII/29, kart. 371.

sign. XVIII/30, kart. 372.

sign. XV/1, kart. 373.

sign. XV/2, kart. 374.

sign. XV/3, kart. 375.

sign. XV/4, kart. 376.

sign. XV/8, kart. 380.

sign. XV/9, kart. 381.

sign. XV/10, kart. 382.

sign. XV/11, kart. 383.

sign. XV/12, kart. 384.

sign. XV/13, kart. 385.

sign. XV/14, kart. 386.

sign. XV/19, kart. 391.

sign. XV/20, kart. 392.

Prameny vydané

POLIŠENSKÝ, Josef (edd). *Der Krieg und die Gesellschaft in Europa 1618-1648*. 1. vydání. Praha: Academia, 1971. Documenta Bohemica bellum tricennale illustrantia.

Literatura

BAUER, Friedrich L. *Historische Notizen zur Informatik*. Berlin: Springer, 2009. ISBN 978-3-540-85790-7.

BISCHOFF, Bernhard. *Übersicht über die nichtdiplomatischen Geheimschriften des Mittleralters*. In: MIÖG 62, 1954, s. 1-27.

DRÖSCHER, Ernst. *Die Methoden der Geheimschriften (Zifferschriften) unter Berücksichtigung ihrer geschichtlichen Entwicklung*. Leipzig: K. F. Koehler, 1921.

ERNST, Hildegard. *Geheimschriften der Habsburger im Dreißigjährigen Krieg*. In: Siglo de Oro – Decadencia. Spaniens Kultur und Politik in der ersten Hälfte des 17. Jahrhunderts, hrsg. von Heinz Duchhardt/Christoph Strosetzki. Köln, Weimar, Wien: Böhlau Verlag, 1996, s. 95-108. ISNB 9783412071967.

ERNST, Hildegard. *Geheimschriften im diplomatischen Briefwechsel zwischen Wien, Madrid und Brüssel 1635-1642*. In: MÖStA Bd. 42, Wien: Ferdinand Berger & Söhne, 1992, s. 102-127. ISNB 3-85028-211-2.

ERNST, Hildegard. *Geheimschriften im diplomatischen Briefwechsel zwischen Wien, Madrid und Brüssel 1635-1642 (Teil II)*. In: MÖStA Bd. 45, Wien: Ferdinand Berger & Söhne, 1997, s. 207-232. ISBN 3-85028-296-1.

FLEISSNER VON WOSTROWITZ, Eduard B. *Handbuch der Kryptographie. Anleitung zum Chiffriren und Dechiffriren von Geheimschriften*. Wien: In Commission bei L. W. Seidel & Sohn, 1881.

FURLARI, Silvio. *La stenografia e la crittografia – scienze ausiliarie della storia*. In: Römische Historische Mitteilungen 31, Wien: VÖAW, 1989, s. 578-589. ISBN 3-7001-1721-3.

GERLICH, Wilhelm. *Die Entzifferung von historischen Geheimschriften*. In: MÖStA Bd. 1. Wien: Österreichische Staatsdruckerei, 1948, s. 445-469.

HLAVÁČEK, Ivan – KAŠPAR, Jaroslav – NOVÝ, Rostislav. *Vademecum pomocných věd historických*. 5. upravené a doplněné vydání. Jinočany: H & H, 2015. ISBN 80-7319-004-4.

HUSA, Václav. *K dějinám nevolnického povstání roku 1775*. In: Český lid. Praha: [Brázda], 1952, roč. 39, č. 11-12, str. 243-255.

HÜTTENHAIN, Erich. *Die Geheimschriften des Fürstbistums Münster unter Christoph Bernhard von Galen 1650-1678*. Münster: Aschendorff, 1974. Schriften der Historischen Kommission Westfalens. ISBN 3402056097.

KAHN, David. *The Codebreakers: the story of secret writting*. New York: Scribner, 1996. ISBN 0-684-83130-9.

KAŠPAR, Jaroslav. *Příspěvek k řešení tajného písma ze 17. století*. In: Acta Universitatis Carolinae: Philosophica et Historica č. 5. Praha: [s.n], 1963, s. 95-107.

KAŠPAR, Jaroslav. *Soubor statí o novověkém písmu*. 1. vydání. Praha: Universita Karlova, 1993, s. 177-209. ISBN 80-7066-679-X.

KILIÁN, Jan. *Jan Matyáš Gallas*. In: Valdštejn: Albrecht z Valdštejna Inter arma silent musae?. Praha: Academia, 2007, s. 287-294. ISBN 978-80-200-1565-5.

KLÍMA, Vlastimil. *Utajené komunikace – 4. díl: Od novověku do 20. století*. In: Chip: počítačový magazín. Praha: Vogel Publishing, 1994, roč. 4, č. 8, s. 118-121.

KLÜBER, Johann Ludwig. *Kryptographik. Lehrbuch der Geheimschreibekunst (Chiffrir- und Dechiffrirkunst) in Staats- und Privatgeschäften*. Tübingen: J. G. Cotta'schen Buchhandlung, 1809.

LICHTNER, Jaromír. *Šifrování. Úvod do kryptografie chemické i grafické se 40 šifrovými klíči*. Praha: Alois Srdce, 1939.

MALOCH, Antonín Vánkomil. *Rozluštění chiffrovaného písma v češtině*. In: Lumír, 1858, roč. 8, č. 9, s. 205-206.

MEISTER, Aloys. *Anfänge der modernen diplomatischen Geheimschrift*. Paderborn: Schöningh Verlag, 1902.

MEISTER, Aloys. *Die Geheimschrift im Dienste der päpstlichen Kurie: von ihren Anfängen bis zum Ende des XVI. Jahrhunderts*. Paderborn: Schöningh Verlag, 1906.

MÍRKA, Jakub. *Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni*. In: Západočeské archivy. Plzeň: Státní oblastní archiv v Plzni, 2012, s. 44-73. ISBN 978-80-904696-3-1.

REBITSCH, Robert. *Matyáš Gallas: (1588–1647). Císařský generál a Valdštějnův „dědic“*. Praha: Grada, 2013. ISBN 978-80-247-4778-1.

ROUBÍK, František. *Šifrované dopisy v registratuře Albrechta z Valdštejna*. In: Sborník prací věnovaných prof. dru Gustavu Friedrichovi k šedesátým narozeninám: 1871-1931. Praha: Historický spolek v Praze, 1931, s. 359-368.

ROUS, Anne-Simone – MULSOW, Martin. *Geheime Post: Kryptologie und Steganographie der diplomatischen Korrespondenz europäischer Höfe während der Frühen Neuzeit*. Berlin: Duncker & Humblot, 2015. ISBN 3428144171.

RYBA, Bohumil. *K tajnému písmu v listech Husových*. In: Sborník historický 1, 1953, s. 46-52.

SMÍŠKOVÁ, Helena. *Historická sbírka (rodinný archiv Clam-Gallasů)*. In: AČ. Praha: Sekce Archivní správy MV ČR, 1994, roč. 44, č. 3, 137-141.

SMÍŠKOVÁ, Helena. *Historická sbírka (rodinný archiv Clam-Gallasů) II. část*. In: AČ. Praha: Sekce Archivní správy MV ČR, 1998, roč. 48, č. 1, 17-23.

SMÍŠKOVÁ, Helena. *Rodinný archiv (Historická sbírka) Clam-Gallas (1238) 1529–1947. Inventář*. Děčín, 1996. ev. č. 1038.

STIX, Franz. *Zur Geschichte und Organisation der Wiener Geheimen Ziffernkanzlei. (Von ihren Anfängen bis zum Jahre 1848.)*. In: MIÖG Bd. 51, Innsbruck: Universitäts-Verlag Wagner, 1937, s. 131-160

VAVROUŠKOVÁ, Anna. *Šifrované dopisy Fridricha Falckého*. Praha: [s. n.], 1933.

VONDRUŠKA, Pavel. *Kryptologie, šifrování a tajná písma*. Praha: Albatros, 2006. Oko. ISBN 80-00-01888-8.

WAGNER, Friedrich. *Studien zu einer Lehre von der Geheimschrift (Chiffernkunde)*. In: Archivalische Zeitschrift Bd. 11 (1886), s. 156-189; Bd. 12 (1887), s. 1-29; Bd. 13 (1888), s. 8-44.

Literatura online

ALLMAYER-BECK, Johann Christoph. *Colloredo-Waldsee, Rudolf Graf von*. In: Neue Deutsche Biographie 3, 1957, s. 328 f. [online]. [cit. 13. 8. 2017]. Dostupné z: `https://www.deutsche-biographie.de/sfz8629.html#ndbcontent`.

BIERTHER, Kathrin. *Piccolomini, Ottavio Fürst*. In: Neue Deutsche Biographie 20, 2001, s. 408-410 [online]. [cit. 5. 8. 2017]. Dostupné z: `https://www.deutsche-biographie.de/sfz95776.html#ndbcontent`.

BROUCEK, Peter. *Leslie, Walter von.* In: Neue Deutsche Biographie 14, 1985, s. 331 f. [online]. [cit. 6. 8. 2017]. Dostupné z: https://www.deutsche-biographie.de/gnd122181220.html#ndbcontent.

FRANZEN, August. *Ferdinand.* In: Neue Deutsche Biograpfie 5, 1961, s. 90 [online]. [cit. 7. 8. 2017]. Dostupné z: https://www.deutsche-biographie.de/sfz56892.html#ndbcontent.

GEISTHARDT, Fritz. *Holzappel, Peter Graf zu.* In: Neue Deutsche Biographie 9, 1972, s. 571 [online]. [cit. 8. 8. 2017]. Dostupné z: https://www.deutsche-biographie.de/sfz33603.html#ndbcontent.

HÜTTL, Ludwig. *Leopold Wilhelm.* In: Neue Deutsche Biographie 14, 1985, s. 296-298 [online]. [cit. 31. 5. 2017]. Dostupné z: https://www.deutsche-biographie.de/gnd118727664.html#ndbcontent.

KLÍMA, Vlatimil. *Základy moderní kryptologie – Symetrická kryptografie I.* [online]. 2005, [cit. 4. 4. 2017]. Dostupné z: http://www.karlin.mff.cuni.cz/~tuma/nciphers/Symetricka_kryptografie_I.pdf.

RIEDENAUER, Erwin. *Kurtz von Senftenau, Ferdinand Sigismund Graf.* In: Neue Deutsche Biographie 13, 1982, s. 328 f. [online]. [cit. 9. 8. 2017]. Dostupné z: https://www.deutsche-biographie.de/sfz47164.html#ndbcontent.

SCHULZE, Heinz-Joachim. *Königsmarck, Hans Christoph Graf von.* In: Neue Deutsche Biographie 12, 1979, s. 360 f. [online]. [cit. 11. 8. 2017]. Dostupné z: https://www.deutsche-biographie.de/sfz43859.html#ndbcontent.

Ostatní zdroje

Portál „Westfälische Geschichte“

Životopisný portrét J. A. Salvia [online]. [cit. 12. 8. 2017]. Dostupné z: http://www.lwl.org/westfaelische-geschichte/portal/Internet/finde/langDatensatz.php?urlID=5505&url_tabelle=tab_person.

Životopisný portrét J. A. Oxenstierny [online]. [cit. 11. 8. 2017]. Dostupné z: http://www.lwl.org/westfaelische-geschichte/portal/Internet/finde/langDatensatz.php?urlID=5504&url_tabelle=tab_person.

Webové stránky MV ČR, sekce Archivnictví a spisová služba

Evidence archivních fondů a sbírek v ČR. Dostupné z: http://aplikace.mvcr.cz/archivni-fondy-cr.

Webové stránky kryptoanalytika Klause Schmeha

Die ungelöste Geheimschrift von Kaiser Ferdinand III. [online]. [cit. 31. 5. 2017]. Dostupné z:
`http://scienceblogs.de/klausis-krypto-kolumne/2014/05/23/die-ungeloeste-geheimschrift-von-kaiser-ferdinand-iii/`.

Webové stránky Universität Erfurt

Program konference „Geheime Post. Kryptologie und Steganographie der diplomatischen Korrespondenz europäischer Höfe während der Frühen Neuzeit“ [online]. [cit. 31. 5. 2017]. Dostupné z:
`https://www.uni-erfurt.de/fileadmin/user-docs/FGE/Veranstaltungen_2013/Tagungen/Geheime_Post/Flyer_Geheime_Post.pdf`.

Seznam obrázků

4.1.1 Počet šifrovaných dopisů v jednotlivých letech. 27

A.2.1 Nomenklátor „císařské“ šifry. 86
A.3.1 Dopis kurfiřta Ferdinanda z 25. června 1635. 89
A.3.2 Část dopisu Waltera Leslieho z 12. července 1644. 90

Seznam tabulek

4.2.1 *Rekonstruovaný šifrovací klíč pro „královskou“ šifru* 29
4.2.2 *Rekonstruovaný šifrovací klíč kurfiřta Ferdinanda* 32
4.2.3 *Stará šifra s Piccolominim* 35
4.2.4 *Nová šifra s Piccolominim* 35
4.2.5 *Rekonstruovaná část šifrovacího klíče W. Leslieho* 37
4.2.6 *Rekonstruovaná část Carettova šifrovacího klíče* 40
4.2.7 *Rekonstruovaná část šifrovacího klíče „Torstensson–Königsmarck“* 43

A.2.1 Možnosti, jak zašifrovat slovo *allen* „císařskou“ šifrou 87
A.2.2 Odpovídající část šifrovacího klíče „císařské“ šifry. 88
A.2.3 Možnosti, jak zašifrovat slovo *allen* „královskou“ šifrou. 88
A.2.4 Odpovídající část šifrovacího klíče „královské“ šifry. 88

A. Přílohy

A.1 Soupis šifrovaných písemností

V následujícím přehledu jsou zaznamenány všechny šifrované písemnosti Gallasovy válečné kanceláře v chronologickém pořadí, které odpovídá jejich uspořádání v rámci fondu. Z tohoto důvodu a také pro větší názornost jsou dopisy ze souboru šifrovaných dopisů a klíčů uvedeny zvlášť na konci soupisu. U jednotlivých písemností je uvedeno několik základních údajů: forma (jedná-li se o originál, kopii či opis), odesílatel,[1] příjemce a jazyk[2] písemnosti. Je-li některý z údajů označen otazníkem, znamená to, že jej nebylo možné určit s jistotou. Chybí-li údaj úplně, pak nebyl určen vůbec.

Podle potřeby jsou navíc u některých písemností doplněny i podrobnější informace, týkající se šifer, souvislostí mezi některými dopisy, aj.

Rok 1634

1. dopis z 22. 8. 1634[3]
    - originál
    - **odesílatel:** Rudolf hrabě Colloredo von Waldsee, císařský generál strážmistr[4]
    - **příjemce:** Matyáš Gallas, hrabě z Kampu a Freyenthurnu, pán na Smiřicích, Liberci a Frýdlantu, skutečný tajný a válečný rada Jeho císařského Majestátu, komorník, generál lajtnant, polní maršál a nejvyšší[5]
    - **jazyk:** italština
2. dopis z 25. 8. 1634
    - **odesílatel:** Rudolf hrabě Colloredo von Waldsee
    - **příjemce:** Matyáš Gallas
    - **jazyk:** italština

[1] U prvního výskytu odesílatele, případně příjemce, pokud to není Matyáš Gallas, je rovněž uvedena hodnost či profese. U dalších dopisů stejného odesílatele se tato informace neopakuje. Chybí-li u některého odesílatele tato informace, znamená to, že jsem ji nedohledala.

[2] Naprostá většina dopisů je šifrována částečně, tzn. že je text prokládán nešifrovanými pasážemi, z nichž je možné určit jazyk písemnosti. Ten jsem navíc ověřila v případech, kdy mi byla šifra známa. Tímto způsobem jsem mohla určit i jazyk několika dopisů, které byly šifrovány celkově. U mnoha dopisů bylo také možné určit jazyk díky dochovanému dešifrovanému textu.

[3] Dopisy č. 1-2: HS Clam-Gallasů, sign. XVIII/5, kart. 347.

[4] Po pádu Valdštejna povýšen do hodnosti polního maršála. Srov. ALLMAYER-BECK, Johann Christoph. *Colloredo-Waldsee, Rudolf Graf von.* In: Neue Deutsche Biographie 3, 1957, s. 328 f. [online]. [cit. 13. 8. 2017]. Dostupné z: `https://www.deutsche-biographie.de/sfz8629.html#ndbcontent`.

[5] Srov. REBITSCH, R. *Matyáš Gallas*, s. 10.
Dále jen Matyáš Gallas.

Rok 1635

3. dopis z 10. 6. 1635[6]
    - **odesílatel:** don Martin Axpes
    - **příjemce:** Christopf Wehr
    - **jazyk:** španělština
4. dopis z 25. 6. 1635
    - kopie (?)
    - **odesílatel:** město Arnsberg (?)
        - v dataci uveden Arnsberg, jako odesílatelé uvedeni „vestfálští radní“ (Westfälische Räte)
    - **příjemce:** Ferdinand von Bayern, kolínský arcibiskup a kurfiřt
    - **jazyk:** němčina
    - připojeno P. S. z 26. 6.
    - příloha dopisu č. 5 (?)
5. dopis z 28. 6. 1635
    - originál (?)
    - **odesílatel:** Ferdinand von Bayern
    - **příjemce:** Matyáš Gallas (?)
    - **jazyk:** němčina
6. dopis z 25. 8. 1635[7]
    - originál
    - **odesílatel:** Ferdinand von Bayern
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
7. dopis z 2. 9. 1635
    - **odesílatel:** Rudolf hrabě Colloredo von Waldsee
    - **příjemce:** Matyáš Gallas
    - **jazyk:** italština
8. dopis z 5. 9. 1635
    - **odesílatel:** Rudolf hrabě Colloredo von Waldsee
    - **příjemce:** Matyáš Gallas
    - **jazyk:** italština

[6] Dopisy č. 3-5: HS Clam-Gallasů, sign. XVIII/6, kart. 348.
[7] Dopisy č. 6-15: tamtéž, sign. XVIII/7, kart. 349.

9. dopis z 22. 9. 1635
    - **odesílatel:** Rudolf hrabě Colloredo von Waldsee
    - **příjemce:** Matyáš Gallas
    - **jazyk:** italština
10. dopis ze září roku 1635, s.d.
    - **jazyk:** italština
11. dopis ze 7. 10. 1635
    - **odesílatel:** Rudolf hrabě Colloredo von Waldsee
    - **příjemce:** Matyáš Gallas
    - **jazyk:** italština
12. dopis z 8. 10. 1635
    - **odesílatel:** Ferdinand III., král český, uherský a chorvatský
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
13. dopis z 15. 10. 1635
    - **odesílatel:** Rudolf hrabě Colloredo von Waldsee
    - **jazyk:** italština
14. dopis z 16. 12. 1635
    - originál
    - **odesílatel:** don Martin Axpes
    - **příjemce:** Matyáš Gallas (?)
    - **jazyk:** španělština
15. protokol z prosince 1635
    - koncept
    - **jazyk:** němčina

Rok 1636

16. dopis z 22. 1. 1636[8]
    - **odesílatel:** Rudolf hrabě Colloredo von Waldsee
    - **příjemce:** Matyáš Gallas
    - **jazyk:** italština

[8] Dopisy č. 16-20: tamtéž, sign. XVIII/8, kart. 350.

17. dopis z 23. 1. 1636
    - **odesílatel:** Rudolf hrabě Colloredo von Waldsee
    - **příjemce:** Matyáš Gallas
    - **jazyk:** italština
18. dopis z ledna roku 1636, s.d.
19. dopis z 13. 4. 1636
    - **odesílatel:** Rudolf hrabě Colloredo von Waldsee
    - **příjemce:** Matyáš Gallas
    - **jazyk:** italština
20. dopis z 20. 7. 1636
    - **odesílatel:** Ottavio Piccolomini, císařský polní maršál
    - **příjemce:** Matyáš Gallas
    - **jazyk:** italština
21. dopis z 27. 8. 1636[9]
    - originál
    - **odesílatel:** označen jako S. A.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** španělština
22. dopis z 25. 9. 1636
    - originál
    - **odesílatel:** král Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
23. dopis z 5. 10. 1636
    - originál
    - **odesílatel:** král Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
24. dopis ze 7. 10. 1636
    - originál
    - **odesílatel:** král Ferdinand III.
    - **příjemce:** Matyáš Gallas

[9] Dopisy č. 21-26: tamtéž, sign. XVIII/9, kart. 351.

- **jazyk:** němčina

25. dopis z 29. 10. 1636
    - kopie
    - zachycený
26. dopis z října roku 1636, s.d.
    - **odesílatel:** Ottavio Piccolomini
    - **příjemce:** Matyáš Gallas
    - **jazyk:** italština
27. dopis z 5. 11. 1636[10]
    - originál
    - **odesílatel:** král Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
28. dopis z 8. 11. 1636
    - originál
    - **odesílatel:** král Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
29. dopis z 15. 11. 1636
    - originál
    - **odesílatel:** král Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
30. dopis z 20. 11. 1636
    - originál
    - **odesílatel:** král Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
31. dopis z 31. 12. 1636
    - **odesílatel:** Rudolf Tiefenbach, císařský polní maršál
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

[10] Dopisy č. 27-33: tamtéž, sign. XVIII/10, kart. 352.

- šifra se shoduje se šifrou Gallas – král Ferdinand III.

32. propozice z 29. 9. 1636

    - koncept
    - ve složce s názvem „Strassburger Traktat 1636 I.“[11]

33. relace z 3. 11. 1636

    - koncept
    - ve složce s názvem „Strassburger Traktat 1636 I.“

Rok 1637

34. dopis z 28. 3. 1637[12]

    - originál
    - **odesílatel:** císař Ferdinand III.[13]
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

35. dopis z 15. 4. 1637

    - **odesílatel:** Francesco Caretto, markýz di Grana, císařský polní zbrojmistr
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

36. dopis z 16. 4. 1637[14]

    - **odesílatel:** Francesco Caretto, markýz di Grana
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

37. dopis 18. 4. 1637

    - **odesílatel:** Francesco Caretto, markýz di Grana
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

38. dopis z 27. 3. 1637

    - přiložen k dopisu z 22. 4. 1637
    - **jazyk:** němčina

[11] Složka obsahuje řadu nešifrovaných písemností. Zatím není jasné, co je přesně jejím obsahem.
[12] Dopisy č. 34-35: HS Clam-Gallasů, sign. XVIII/11, kart. 353.
[13] Od února 1637 je Ferdinand III. císařem. Srov. REBITSCH, R. *Matyáš Gallas*, s. 230.
[14] Dopisy č. 36-42: HS Clam-Gallasů, sign. XVIII/12, kart. 354.

39. dopis z 24. 4. 1637
    - **odesílatel:** Francesco Caretto, markýz di Grana
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
40. dopis z 28. 4. 1637
    - **odesílatel:** Francesco Caretto, markýz di Grana
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
41. dopis z 30. 4. 1637
    - **odesílatel:** Francesco Caretto, markýz di Grana
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
42. dopis z 5. 6. 1637
    - **jazyk:** latina

Rok 1638

43. výtah z dopisu z 18. 7. 1638[15]
    - šifra se shoduje se šifrou Gallas–Caretto–Kurtz
    - **jazyk:** němčina
44. koncept, s. d.
    - nachází se ve složce několika dopisů
    - součástí konceptu jsou malé šifrované části, slepené v jeden celek
    - na jednom z dopisů je označen hrabě Kurtz, s nímž Matyáš Gallas užíval stejnou šifru jako s markýzem Carettem di Grana
    - šifra v konceptu se shoduje se šifrou Gallas–Caretto–Kurtz
    - **jazyk:** němčina
45. dopis z 28. 7. 1638
    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

[15] Dopisy č. 43-47: tamtéž, sign. XVIII/18, kart. 360.

46. koncept z 8. 8. 1638

    - **jazyk:** italština
    - šifra v konceptu se shoduje se šifrou Gallas–Caretto–Kurtz

47. výtah z rezoluce (Substantia der kpnig[lichen][16] dennemarkh[ischen] resolution)

    - **praesentatum na reversu:** 25. 8. 1638
    - **odesílatel:** Ferdinand Zikmund hrabě Kurtz von Senftenau, říšský vicekancléř
    - **příjemce:** Matyáš Gallas (?)
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas–Caretto–Kurz

48. dopis z 13. 11. 1638[17]

    - **odesílatel:** Rudolf hrabě Colloredo von Waldsee
    - **příjemce:** Matyáš Gallas
    - **jazyk:** italština

Rok 1639

49. dopis z 11. 5. 1639[18]

    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Jindřich Šlik z Holíče a Pasounu, prezident dvorské rady válečné
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas – král Ferdinand III.

Rok 1643

50. dopis z 28. 1. 1643[19]

    - obsahuje šifrovanou přílohu
    - **odesílatel:** Ottavio Piccolomini
    - **příjemce:** Matyáš Gallas
    - **jazyk:** italština

[16] Dešifrováno z úvodu zprávy. Ve slově „königlichen“ překlep šifranta.
[17] HS Clam-Gallasů, sign. XVIII/19, kart. 361.
[18] Tamtéž, sign. XVIII/20, kart. 362.
[19] Dopisy č. 50-51: tamtéž, sign. XVIII/23, kart. 365.

51. dopis, s. d.

    - přiložen u dopisu saského kurfiřta Jana Jiřího I. Ottaviu Piccolominimu z 21. 3. 1643
    - **jazyk:** němčina

52. dopis ze 17. 6. 1643[20]

    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

53. výtah z dopisu z 18. 6. 1643

    - **odesílatel dopisu:** Francesco Caretto, markýz di Grana
    - **příjemce:** císař Ferdinand III.
    - **jazyk:** němčina
    - zašifrovaný extrakt přiložen k dopisu Francesca Caretta Matyáši Gallasovi ze dne 23. 6. 1643
    - přiložen i duplikát extraktu

54. výtah z dopisu z 18. 6. 1643

    - není totožný s dopisem č. 53
    - **odesílatel dopisu:** Francesco Caretto, markýz di Grana
    - **příjemce:** císař Ferdinand III.
    - **jazyk:** němčina
    - zašifrovaný extrakt přiložen k dopisu Francesca Caretta Matyáši Gallasovi ze dne 23. 6. 1643
    - přiložen i duplikát extraktu

55. dopis z 29. 6. 1643

    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

56. dopis z 4. 7. 1643[21]

    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

[20] Dopisy č. 52-55: tamtéž, sign. XVIII/27, kart. 369.
[21] Dopisy č. 56-59: tamtéž, sign. XVIII/28, kart. 370.

57. dopis z 9. 7. 1643

    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

58. dopis z 14. 7. 1643

    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

59. dopis z 16. 7. 1643

    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

60. dopis z 11. 8. 1643[22]

    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

61. dopis z 12. 8. 1643

    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

62. dopis z 18. 8. 1643

    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

63. dopis z 26. 8. 1643

    - příloha dopisu Ferdinanda III. Matyáši Gallasovi z 29. 8. 1643 (?)
    - **odesílatel:** György Lippay, arcibiskup ostřihomský

[22] Dopisy č. 60-63: tamtéž, sign. XVIII/29, kart. 371.

- **příjemce:** císař Ferdinand III.
- **jazyk:** latina
- šifra se shoduje se šifrou Gallas – císař Ferdinand III.

64. dopis z 1. 9. 1643[23]

- **odesílatel:** Johann hrabě von Götzen, císařský polní maršál
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

65. dopis z 2. 9. 1643

- originál
- **odesílatel:** císař Ferdinand III.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

66. dopis z 4. 9. 1643

- originál
- **odesílatel:** císař Ferdinand III.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina
- přiložen i duplikát dopisu

67. dopis z 5. 9. 1643

- originál
- **odesílatel:** císař Ferdinand III.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

68. dopis z 5. 9. 1643

- není totožný s dopisem č. 67
- originál
- **odesílatel:** císař Ferdinand III.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

69. dopis z 6. 9. 1643

- originál
- **odesílatel:** císař Ferdinand III.

[23] Dopisy č. 64-73: tamtéž, sign. XVIII/30, kart. 372.

- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

70. dopis ze 14. 9. 1643

    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

71. dopis z 25. 9. 1643

    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

72. dopis z 25. 9. 1643

    - ve dvou šifrovaných vyhotoveních, označených jako duplikát a triplikát
    - **odesílatel:** Johann hrabě von Götzen
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

73. dopis z 27. 9. 1643

    - **odesílatel:** Johann hrabě von Götzen
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
    - v příloze duplikát a triplikát

74. dopis z 4. 10. 1643[24]

    - originál
    - **odesílatel:** Johann hrabě von Götzen
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

75. dopis z 11. 10. 1643

    - originál
    - **odesílatel:** Johann hrabě von Götzen
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

[24] Dopisy č. 74-90: tamtéž, sign. XV/1, kart. 373.

76. dopis z 14. 10. 1643
    - **odesílatel:** Mathieu Vernier
    - **jazyk:** francouzština
77. dopis z 20. 10. 1643
    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
78. dopis z 21. 9. 1643
    - příloha dopisu č. 77.
    - **odesílatel:** Johann Ernst Krackhau, generál strážmistr
    - **příjemce:** císař Ferdinand III.
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas – císař Ferdinand III.
79. dopis z 25. 9. 1643
    - příloha dopisu č. 77
    - kopie
    - **odesílatel:** Johann Ernst Krackhau
    - **příjemce:** hrabě Šlik
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas – císař Ferdinand III.
80. dopis z 26. 9. 1643
    - příloha dopisu č. 77
    - kopie
    - **odesílatel:** Johann Ernst Krackhau
    - **příjemce:** hrabě Šlik
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas – císař Ferdinand III.
81. dopis z 12. 10. 1643
    - příloha dopisu č. 77
    - **odesílatel:** Schmaltz, sekretář J. E. Krackhaua (?)
    - **příjemce:** císař Ferdinand III.
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas – císař Ferdinand III.

82. dopis z 20. 10. 1643
    - příloha dopisu č. 77
    - kopie
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Johann Ernst Krackhau
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas – císař Ferdinand III.
83. dopis z 21. 10. 1643
    - **odesílatel:** Mathieu Vernier
    - **jazyk:** francouzština
84. Post scriptum, s. d.
    - originál (?)
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
85. dopis z 27. 10. 1643
    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
86. dopis z 27. 10. 1643
    - příloha dopisu č. 85
    - **odesílatel:** Johann Ernst Krackhau
        - v katalogu korespondentů M. Gallasovi je na záznamu Krackhaua k tomuto dopisu uvedeno, že byl podán císaři prostřednictvím sekretáře Schmaltze (Eingabe durch Sekr[etär] Schmaltz an Ferd. III.)
    - **příjemce:** Ferdinand III.
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas – císař Ferdinand III.
87. dopis z 27. 10. 1643
    - není totožný s dopisem č. 85
    - originál
    - **odesílatel:** císař Ferdinand III.

- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

88. dopis z 28. 10. 1643

    - dopis je součástí složky s dvěma (nešifrovanými) kopiemi dopisů Ferdinanda III. generál strážmistrovi Krackhauovi (z 28. a 29. 10. 1643)
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

89. dopis z 29. 10. 1643

    - **odesílatel:** Mathieu Vernier
    - **jazyk:** francouzština

90. dopis z 29. 10. 1643

    - není totožný s dopisem č. 89
    - **odesílatel:** Mathieu Vernier
    - **jazyk:** francouzština

91. dopis z 5. 11. 1643[25]

    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

92. dopis z 5. 11. 1643

    - příloha dopisu č. 91
    - kopie
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Johann Ernst Krackhau
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas – císař Ferdinand III.

93. dopis z 9. 11. 1643

    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

[25] Dopisy č. 91-95: tamtéž, sign. XV/2, kart. 374.

94. dopis, s. d.

    - kopie
    - spolu s několika dalšími (nešifrovanými) dopisy přiložen k dopisu č. 93
    - šifra se shoduje se šifrou Gallas – císař Ferdinand III.

95. dopis z 30. 11. 1643

    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

96. dopis z 2. 12. 1643[26]

    - dopis se skládá ze dvou dopisů ve dvou jazycích
    - **oba dopisy:** kopie
    - **jazyk:** italština, španělština
    - **odesílatel první části, psané v italštině:** markýz de Torrdelaguna
    - v obou částech se šifra shoduje se šifrou Gallas – císař Ferdinand III. pro korespondenci v němčině

97. dopis z 6. 12. 1643

    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

98. dopis z 12. 12. 1643

    - **odesílatel:** markýz de Torrdelaguna
    - **příjemce:** císař Ferdinand III.
    - **jazyk:** latina
    - šifra se shoduje se šifrou Gallas – císař Ferdinand III. pro korespondenci v němčině

99. propozice z 12. 12. 1643

    - příloha dopisu č. 98
    - **jazyk:** španělština
    - šifra se shoduje se šifrou Gallas – císař Ferdinand III. pro korespondenci v němčině

[26] Dopisy č. 96-99: tamtéž, sign. XV/3, kart. 375.

Rok 1644

100. dopis z 1. 1. 1644[27]

    - originál
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
    - šifra se shoduje se šifrou, kterou užíval Matyáš Gallas v korespondenci s Wilhelmem Leopoldem von Tattenbach

101. dopis z 20. 1. 1644

    - **jazyk:** italština

102. dopis z 29. 5. 1644[28]

    - jedná se o jednu z příloh dopisu z 23. 6. 1644, adresovaného Matyáši Gallasovi, v záležitosti odchyceného dopisu nepřítele
    - ve dvou vyhotoveních
    - **jazyk:** němčina

103. dopis z 11. 7. 1644[29]

    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

104. dopis z 12. 7. 1644

    - **odesílatel:** Walter Leslie, císařský plukovník
    - **jazyk:** italština

105. dopis ze 14. 7. 1644

    - zachycený dopis
    - originál
    - **odesílatel:** Lennart Torstensson, švédský polní maršál
    - **příjemce:** Johan Axelsson Oxenstierna, švédský vyslanec
    - **jazyk:** švédština

106. dopis z 15. 7. 1644

    - zachycený dopis
    - kopie

[27] Dopisy č. 100-101: tamtéž, sign. XV/4, kart. 376.
[28] Tamtéž, sign. XV/8, kart. 380.
[29] Dopisy č. 103-111: tamtéž, sign. XV/9, kart. 381.

- **odesílatel:** Alexander Erskin, švédský královský rada
- **příjemce:** Johann Adler Salvius, švédský diplomat
- **jazyk:** němčina

107. dopis z 26. 7. 1644

- originál
- **odesílatel:** císař Ferdinand III.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina
- obsahuje 3 přílohy (A, B, C), z nichž dvě jsou rovněž šifrované

108. memoriál, s. d.

- příloha A dopisu č. 107
- opis
- **odesílatel:** hrabě de Saint Amour
- **příjemce:** císař Ferdinand III.
- **jazyk:** španělština
- šifra se shoduje se šifrou Gallas – císař Ferdinand III. pro korespondenci v němčině

109. dopis ze 17. 5. 1644

- příloha B dopisu č. 107
- opis
- **odesílatel:** Filip IV., španělský král
- **příjemce:** císař Ferdinand III.
- **jazyk:** španělština
- šifra se shoduje se šifrou Gallas – císař Ferdinand III. pro korespondenci v němčině

110. dopis z 28. 7. 1644

- opis
- **odesílatel:** Friedrich Mosser von Filsek (?), würtemberský generál
- **příjemce:** Lennart Torstensson
- **jazyk:** němčina

111. dopis z 23. 7. 1644

- originál
- **odesílatel:** hrabě von Auersperg
- **příjemce:** Matyáš Gallas

- **jazyk:** němčina

112. dopis z 9. 8. 1644[30]

    - **odesílatel:** Georg von Plettenberg, císařský vyslanec a dvorský válečný rada
    - **příjemce:** Matyáš Gallas (?)
    - **jazyk:** němčina

113. dopis z 9. 8. 1644

    - **odesílatel:** Wilhelm Leopold von Tattenbach, císařský tajný rada, komorník a vyslanec
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina, italština (přípisek)

114. dopis z 13. 8. 1644

    - **odesílatel:** Georg von Plettenberg
    - **příjemce:** Matyáš Gallas (?)
    - **jazyk:** němčina

115. dopis z 16. 8 1644

    - **odesílatel:** Georg von Plettenberg
    - **příjemce:** Matyáš Gallas (?)
    - **jazyk:** němčina (dopis), italština (P. S.)

116. dopis z 23. 8. 1644

    - označeno jako duplikát
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

117. dopis z 24. 8 1644

    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

118. dopis z 25. 8. 1644

    - **odesílatel:** Sigismund Heußner von Wandersleben, císařský válečný komisař

[30] Dopisy č. 112-121: tamtéž, sign. XV/10, kart. 382.

- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

119. dopis z 25. 8. 1644

- není totožný s dopisem č. 118
- **odesílatel:** Sigismund Heußner von Wandersleben
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

120. dopis z 26. 8. 1644

- zachycený dopis
- duplikát
- **odesílatel:** Lennart Torstensson
- **příjemce:** Hans Christoph von Königsmarck, švédský generál major
- **jazyk:** němčina

121. dopis z 30. 8. 1644

- originál
- **odesílatel:** císař Ferdinand III.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina
- přiložen i duplikát

122. dopis z 3. 9. 1644[31]

- **odesílatel:** císař Ferdinand III.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina
- přiložen i duplikát

123. dopis z 3. 9. 1644

- **odesílatel:** Georg von Plettenberg (Giorgio á Plettenberg)
- **příjemce:** Matyáš Gallas (?)
- **jazyk:** italština

124. dopis z 8. 9. 1644

- **odesílatel:** císař Ferdinand III.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

[31] Dopisy č. 122-135: tamtéž, sign. XV/11, kart. 383.

125. dopis z 10. 9. 1644

- originál
- **odesílatel:** císař Ferdinand III.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

126. dopis z 22. 10. 1644

- přiloženo u dopisu č. 125
- **v hlavičce:** „Pro saské kurfiřství, v Linci dne 22. října 1644“ (An zuhr Chur Sachsen de dato Linz von 22. Octobris Anno sechzehenhundertvierundvierzig)[32]
- dopis šifrován celý
- šifra se shoduje se šifrou Gallas – císař Ferdinand III.

127. dopis z 31. 8. 1644[33]

- **odesílatel:** Jan Jiří I., saský kurfiřt
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

128. dopis z 15. 9. 1644

- **odesílatel:** Wilhelm Leopold von Tattenbach
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina
- na samostatném listu přiloženo Post scriptum, které je rovněž zčásti šifrováno

129. dopis, s. d.

- spolu s několika dalšími (nešifrovanými) dopisy přiložen u dopisu č. 128
- **jazyk:** němčina (nešifrovaná část dopisu), italština (šifrovaná část dopisu)
- šifra se shoduje se šifrou Gallas–Tattenbach pro korespondenci v němčině

[32] Dešifrováno na základě dochovaného šifrovacího klíče. Při dešifrování jsem zachovala jednotlivá písmena tak, jak odpovídají šifrovému textu s tím, že jsem použila současný pravopis. V 17. století totiž pravopis nebyl ustálen a není tedy jasné, jak by přesně vypadal dobový dešifrovaný text.

Vzhledem k datu dopisu č. 125 je možné, že k němu byl dopis č. 126 přiložen omylem během pořádání fondu a oba uvedené dopisy spolu nijak nesouvisí. Zatím to ale nemohu potvrdit, ani vyvrátit, takže jsem jej ponechala v řazení na tomto místě.

[33] V registratuře uložen pod datem 10. 9. 1644.

130. dopis ze 17. 9. 1644

- **odesílatel:** císař Ferdinand III.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

131. dopis ze 17. 9. 1644

- **odesílatel:** Georg von Plettenberg
- **příjemce:** Matyáš Gallas (?)
- **jazyk:** němčina

132. dopis z 20. 9. 1644

- **odesílatel:** císař Ferdinand III.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

133. dopis z 23. 9. 1644

- rekoncept
- **odesílatel:** Matyáš Gallas
- **příjemce:** císař Ferdinand III.
- **jazyk:** němčina

134. dopis z 25. 9. 1644

- rekoncept
- **odesílatel:** Matyáš Gallas
- **příjemce:** císař Ferdinand III.
- **jazyk:** němčina
- přiložen i samotný koncept

135. dopis z 30. 9. 1644

- **odesílatel:** Wilhelm Leopold von Tattenbach
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

136. dopis ze 4. 10. 1644[34]

- **odesílatel:** Wilhelm Leopold von Tattenbach
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

[34] Dopisy č. 136-161: HS Clam-Gallasů, sign. XV/12, kart. 384.

137. dopis z 6. 10. 1644
    - **odesílatel:** Wilhelm Leopold von Tattenbach
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
138. dopis z 6. 10. 1644
    - šifra se shoduje se šifrou Gallas–Tattenbach
139. dopis z 1. 10. 1644
    - ve složce spolu s dopisem č. 138
    - **příjemce:** vévoda brunšvicko-lüneburský
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas–Tattenbach
140. dopis z 9. 10. 1644
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
141. dopis z 9. 10. 1644
    - **odesílatel:** Wilhelm Leopold von Tattenbach
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
    - na samostatném listu přiloženo Post scriptum, které je rovněž zčásti šifrováno
142. dopis z 13. 10. 1644
    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
143. dopis z 2. 10. 1644
    - přiložen k dopisu č. 142
    - kopie
    - **odesílatel:** Adrian hrabě Enkevort, císařský polní maršál
    - **příjemce:** císař Ferdinand III.
    - **jazyk:** italština
    - šifra se shoduje se šifrou Gallas – císař Ferdinand III. pro korespondenci v němčině

144. dopis z 13. 10. 1644
    - není totožný s dopisem č. 142
    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
145. dopis z 15. 10. 1644
    - **odesílatel:** Georg von Plettenberg
    - **příjemce:** Matyáš Gallas (?)
    - **jazyk:** němčina
146. dopis z 16. 10. 1644
    - **odesílatel:** Adrian hrabě Enkevort
    - **příjemce:** Matyáš Gallas
    - **jazyk:** italština
147. dopis z 21. 10. 1644
    - **odesílatel:** Wilhelm Leopold von Tattenbach
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
148. dopis z 15. 9. 1644
    - přiloženo k dopisu č. 147
    - kopie
    - **odesílatel:** Wilhelm Leopold von Tattenbach
    - **příjemce:** vévoda brunšvicko-lüneburský
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas–Tattenbach
149. dopis z 7. 10. 1644
    - přiloženo k dopisu č. 147
    - kopie
    - **odesílatel:** město Goslar
    - **příjemce:** Wilhelm Leopold von Tattenbach
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas–Tattenbach

150. dopis z 21. 10. 1644

    - přiloženo k dopisu č. 147
    - kopie
    - **odesílatel:** Wilhelm Leopold von Tattenbach
    - **příjemce:** město Goslar
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas–Tattenbach

151. propozice, s. d.

    - přiloženo k dopisu č. 147
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas–Tattenbach

152. dopis z 22. 10. 1644

    - **odesílatel:** Adrian hrabě Enkevort
    - **příjemce:** Matyáš Gallas
    - **jazyk:** italština (šifrovaný dopis, nešifrovaný přípis na konci dopisu), němčina (oslovení, závěr dopisu: „A zůstávám, Vaše Excelence“ (Und verbleibe, Euer Excell[enz]))

153. dopis z 22. 10. 1644

    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

154. dopis z 23. 10. 1644

    - **odesílatel:** Sigismund Heußner von Wandersleben
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

155. dopis z 23. 10. 1644

    - **odesílatel:** Adrian hrabě Enkevort
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina (nešifrovaná část), italština (šifrovaná část) (?)

156. dopis z 24. 10. 1644

    - **odesílatel:** Adrian hrabě Enkevort
    - **příjemce:** Matyáš Gallas
    - **jazyk:** italština

157. dopis z 25. 10. 1644

- originál
- **odesílatel:** císař Ferdinand III.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

158. dopis z 16. 10. 1644[35]

- originál
- **odesílatel:** Jan Jiří I.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

159. dopis z 26. 10. 1644

- **odesílatel:** Wilhelm Leopold von Tattenbach
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

160. dopis z 28. 10. 1644

- originál
- **odesílatel:** Jan Jiří I.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

161. dopis z 29. 10. 1644

- **odesílatel:** Georg von Plettenberg
- **příjemce:** Matyáš Gallas (?)
- **jazyk:** němčina

162. dopis z roku 1644, s.d.[36]

- šifra se shoduje se šifrou Gallas – císař Ferdinand III.

163. dopis z 1. 11. 1644

- **odesílatel:** Wilhelm Leopold von Tattenbach
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

[35] V registratuře uložen u písemnosti s datem 26. 10. 1644, což je pravděpodobně dešifrovaný dopis z 16. 10. 1644.

[36] Dopisy č. 162-188: HS Clam-Gallasů, sign. XV/13, kart. 385.

164. dopis z 2. 11. 1644

    - originál
    - **odesílatel:** císař Ferdinand III.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

165. dopis z 3. 11. 1644

    - **odesílatel:** Wilhelm Leopold von Tattenbach
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
    - přiložen i duplikát

166. dopis z 21. 10. 1644

    - přiložen k dopisu č. 165
    - kopie ve dvou vyhotoveních
    - **odesílatel:** město Goslar
    - **příjemce:** Wilhelm Leopold von Tattenbach
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas–Tattenbach

167. dopis z 3. 11. 1644

    - přiloženo k dopisu č. 165
    - kopie ve dvou vyhotoveních
    - **odesílatel:** Wilhelm Leopold von Tattenbach
    - **příjemce:** město Goslar
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas–Tattenbach

168. dopis ze 4. 11. 1644

    - přiloženo k dopisu č. 165
    - kopie
    - **odesílatel:** Jacomo de Columbo
    - **příjemce:** město Braunschweig
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas–Tattenbach

169. Post scriptum z 6. 11. 1644

    - dodatek k dopisu č. 165
    - **odesílatel:** Wilhelm Leopold von Tattenbach

- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

170. Post scriptum, s. d.

- přiloženo k dopisu č. 165
- **odesílatel:** Wilhelm Leopold von Tattenbach
- **příjemce:** Matyáš Gallas (?)
- **jazyk:** němčina
- přiložen i duplikát

171. dopis z 8. 11. 1644

- obsahuje i šifrované P. S. z 12. 11. 1644
- **odesílatel:** Georg von Plettenberg
- **příjemce:** Matyáš Gallas (?)
- **jazyk:** němčina, italština

172. dopis z 11. 11. 1644

- originál
- **odesílatel:** císař Ferdinand III.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

173. dopis z 1. 11. 1644[37]

- **odesílatel:** Jan Jiří I.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

174. dopis z 19. 11. 1644

- obsahuje Post scriptum, které je šifrované
- **odesílatel:** Wilhelm Leopold von Tattenbach
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

175. dopis z 19. 11. 1644

- **odesílatel:** Georg von Plettenberg
- **příjemce:** Matyáš Gallas (?)
- **jazyk:** němčina

[37] V registratuře uložen pod datem 11. 11. 1644.

176. dopis z 23. 11. 1644

- šifrovaný je dopis i přiložené Post scriptum
- **odesílatel:** Wilhelm Leopold von Tattenbach
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina
- přiložen i duplikát

177. dopis z 24. 11. 1644

- originál
- **odesílatel:** císař Ferdinand III.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina
- přiložen i duplikát

178. dopis z 3. 12. 1644

- **odesílatel:** Georg von Plettenberg
- **příjemce:** Matyáš Gallas (?)
- **jazyk:** němčina (nešifrovaná část), italština (šifrovaná část)

179. dopis ze 4. 12. 1644

- **odesílatel:** Wilhelm Leopold von Tattenbach
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

180. dopis ze 7. 12. 1644

- **odesílatel:** Melchior hrabě Hatzfeld, císařský polní maršál
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina
- přiložen i duplikát

181. dopis z 28. 11. 1644[38]

- originál ve dvou vyhotoveních
- **odesílatel:** Jan Jiří I.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

182. dopis z 9. 12. 1644

- **odesílatel:** císař Ferdinand III.

[38] V registratuře uložen pod datem 8. 12. 1644.

- **příjemce:** Matyáš Gallas
- **jazyk:** němčina
- přiložen i duplikát a triplikát

183. dopis z 11. 12. 1644

- originál
- **odesílatel:** Jan Jiří I.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

184. dopis z 8. 12. 1644[39]

- originál
- **odesílatel:** Jan Jiří I.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

185. dopis z 20. 12. 1644

- označen jako duplikát
- **odesílatel:** Melchior hrabě Hatzfeld
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina

186. dopis z 21. 12. 1644

- vloženo do dopisu č. 185, ale pravděpodobně spolu oba dopisy nesouvisí
- originál
- **odesílatel:** císař Ferdinand III.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina
- přiložen i duplikát a triplikát

187. dopis z 30. 12. 1644

- originál
- **odesílatel:** císař Ferdinand III.
- **příjemce:** Matyáš Gallas
- **jazyk:** němčina
- přiložen i duplikát, triplikát a quadriplikát

188. dopis z 31. 12. 1644

- **odesílatel:** Georg von Plettenberg
- **příjemce:** Matyáš Gallas (?)
- **jazyk:** němčina (nešifrovaná část), italština (šifrovaná část)

[39] V registratuře uložen pod datem 18. 12. 1644.

Rok 1645

189. dopis z 12. 1. 1645[40]

    - originál
    - **odesílatel:** Carl Fridrich Reich, císařský generální ubytovatel
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

190. dopis z 5. 1. 1645

    - **odesílatel:** Melchior hrabě Hatzfeld
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina
    - přiložen i duplikát

191. dopis z 18. 1. 1645

    - **odesílatel:** Carl Fridrich Reich
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

192. dopis z 28. 1. 1645

    - originál
    - **odesílatel:** Carl Fridrich Reich
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

Složka „Šifrované dopisy + klíče“

193. dopis z 25. 4. 1637[41]

    - **odesílatel:** Francesco Caretto, markýz di Grana
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

194. dopis z 13. 5. 1637

    - originál
    - **odesílatel:** označen jako S. A.
    - **příjemce:** Matyáš Gallas
    - **jazyk:** španělština
    - šifrovací klíč dochován

[40] Dopisy č. 189-192: HS Clam-Gallasů, sign. XV/14, kart. 386.
[41] Dopisy č. 193-201: tamtéž, sign. XV/20, kart. 392.

195. dopis z 23. 6. 1637

    - **odesílatel:** Francesco Caretto, markýz di Grana
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

196. dopis z 3. 9. 1644

    - **odesílatel:** Marches de Leganess
    - **příjemce:** Matyáš Gallas
    - **jazyk:** španělština

197. dopis, s. d.

    - pravděpodobně se jedná o přílohu dopisu č. 196
    - totožná šifra i jazyk

198. dopis z 24. 11. 1644

    - **odesílatel:** označen jako Friederich
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas–Tattenbach

199. Post scriptum, s. d.

    - pravděpodobně rok 1644
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas–Tattenbach

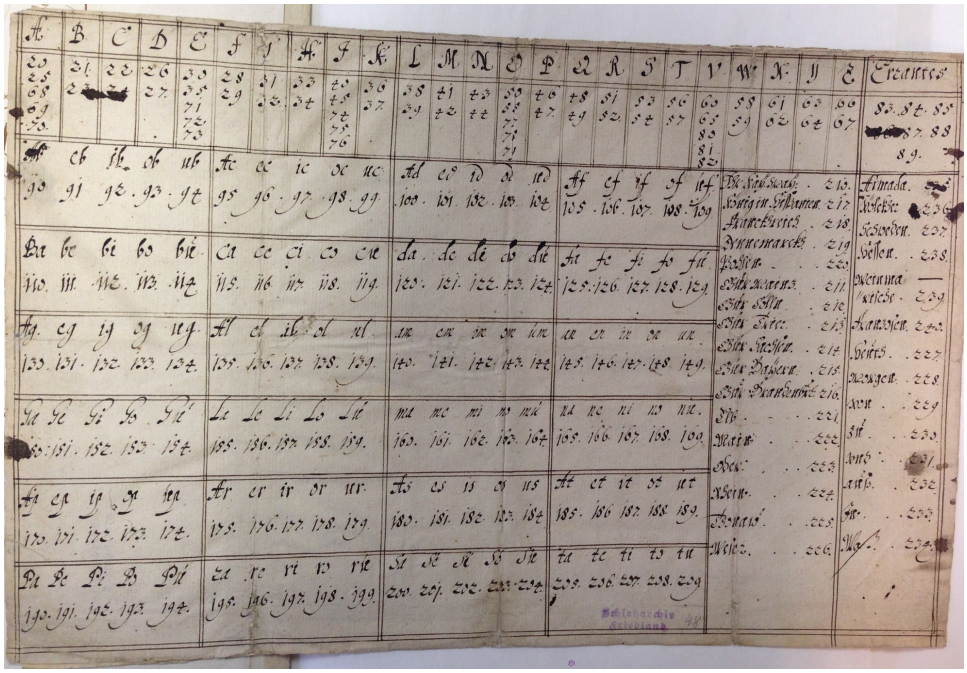
200. dopis z 13. 12. 1644

    - kopie
    - **odesílatel:** Wilhelm Leopold von Tattenbach
    - **příjemce:** kníže-arcibiskup brémský (?)
    - **jazyk:** němčina
    - šifra se shoduje se šifrou Gallas–Tattenbach

201. dopis z 16. 12. 1644

    - **odesílatel:** Wilhelm Leopold von Tattenbach
    - **příjemce:** Matyáš Gallas
    - **jazyk:** němčina

A.2 Příloha k šifrám pro korespondenci Gallase s císařem



Obrázek A.2.1: Nomenklátor „císařské“ šifry.

20 38 38 30 43	20 38 38 30 44	20 38 38 35 43	20 38 38 35 44	20 38 38 71 43	20 38 38 71 44	20 38 38 72 43
20 38 38 72 44	20 38 38 73 43	20 38 38 73 44	20 38 38 146	20 38 39 30 43	20 38 39 30 44	20 38 39 35 43
20 38 39 35 44	20 38 39 71 43	20 38 39 71 44	20 38 39 72 43	20 38 39 72 44	20 38 39 73 43	20 38 39 73 44
20 38 39 146	20 38 156 43	20 38 156 44	20 39 38 30 43	20 39 38 30 44	20 39 38 35 43	20 39 38 35 44
20 39 38 71 43	20 39 38 71 44	20 39 38 72 43	20 39 38 72 44	20 39 38 73 43	20 39 38 73 44	20 39 38 146
20 39 39 30 43	20 39 39 30 44	20 39 39 35 43	20 39 39 35 44	20 39 39 71 43	20 39 39 71 44	20 39 39 72 43
20 39 39 72 44	20 39 39 73 43	20 39 39 73 44	20 39 39 146	20 39 156 43	20 39 156 44	25 38 38 30 43
25 38 38 30 44	25 38 38 35 43	25 38 38 35 44	25 38 38 71 43	25 38 38 71 44	25 38 38 72 43	25 38 38 72 44
25 38 38 73 43	25 38 38 73 44	25 38 38 146	25 38 39 30 43	25 38 39 30 44	25 38 39 35 43	25 38 39 35 44
25 38 39 71 43	25 38 39 71 44	25 38 39 72 43	25 38 39 72 44	25 38 39 73 43	25 38 39 73 44	25 38 39 146
25 38 156 43	25 38 156 44	25 39 38 30 43	25 39 38 30 44	25 39 38 35 43	25 39 38 35 44	25 39 38 71 43
25 39 38 71 44	25 39 38 72 43	25 39 38 72 44	25 39 38 73 43	25 39 38 73 44	25 39 38 146	25 39 39 30 43
25 39 39 30 44	25 39 39 35 43	25 39 39 35 44	25 39 39 71 43	25 39 39 71 44	25 39 39 72 43	25 39 39 72 44
25 39 39 73 43	25 39 39 73 44	25 39 39 146	25 39 156 43	25 39 156 44	68 38 38 30 43	68 38 38 30 44
68 38 38 35 43	68 38 38 35 44	68 38 38 71 43	68 38 38 71 44	68 38 38 72 43	68 38 38 72 44	68 38 38 73 43
68 38 38 73 44	68 38 38 146	68 38 39 30 43	68 38 39 30 44	68 38 39 35 43	68 38 39 35 44	68 38 39 71 43
68 38 39 71 44	68 38 39 72 43	68 38 39 72 44	68 38 39 73 43	68 38 39 73 44	68 38 39 146	68 38 156 43
68 38 156 44	68 39 38 30 43	68 39 38 30 44	68 39 38 35 43	68 39 38 35 44	68 39 38 71 43	68 39 38 71 44
68 39 38 72 43	68 39 38 72 44	68 39 38 73 43	68 39 38 73 44	68 39 38 146	68 39 39 30 43	68 39 39 30 44
68 39 39 35 43	68 39 39 35 44	68 39 39 71 43	68 39 39 71 44	68 39 39 72 43	68 39 39 72 44	68 39 39 73 43
68 39 39 73 44	68 39 39 146	68 39 156 43	68 39 156 44	69 38 38 30 43	69 38 38 30 44	69 38 38 35 43
69 38 38 35 44	69 38 38 71 43	69 38 38 71 44	69 38 38 72 43	69 38 38 72 44	69 38 38 73 43	69 38 38 73 44
69 38 38 146	69 38 39 30 43	69 38 39 30 44	69 38 39 35 43	69 38 39 35 44	69 38 39 71 43	69 38 39 71 44
69 38 39 72 43	69 38 39 72 44	69 38 39 73 43	69 38 39 73 44	69 38 39 146	69 38 156 43	69 38 156 44
69 39 38 30 43	69 39 38 30 44	69 39 38 35 43	69 39 38 35 44	69 39 38 71 43	69 39 38 71 44	69 39 38 72 43
69 39 38 72 44	69 39 38 73 43	69 39 38 73 44	69 39 38 146	69 39 39 30 43	69 39 39 30 44	69 39 39 35 43
69 39 39 35 44	69 39 39 71 43	69 39 39 71 44	69 39 39 72 43	69 39 39 72 44	69 39 39 73 43	69 39 39 73 44
69 39 39 146	69 39 156 43	69 39 156 44	70 38 38 30 43	70 38 38 30 44	70 38 38 35 43	70 38 38 35 44
70 38 38 71 43	70 38 38 71 44	70 38 38 72 43	70 38 38 72 44	70 38 38 73 43	70 38 38 73 44	70 38 38 146
70 38 39 30 43	70 38 39 30 44	70 38 39 35 43	70 38 39 35 44	70 38 39 71 43	70 38 39 71 44	70 38 39 72 43
70 38 39 72 44	70 38 39 73 43	70 38 39 73 44	70 38 39 146	70 38 156 43	70 38 156 44	70 39 38 30 43
70 39 38 30 44	70 39 38 35 43	70 39 38 35 44	70 39 38 71 43	70 39 38 71 44	70 39 38 72 43	70 39 38 72 44
70 39 38 73 43	70 39 38 73 44	70 39 38 146	70 39 39 30 43	70 39 39 30 44	70 39 39 35 43	70 39 39 35 44
70 39 39 71 43	70 39 39 71 44	70 39 39 72 43	70 39 39 72 44	70 39 39 73 43	70 39 39 73 44	70 39 39 146
70 39 156 43	70 39 156 44	135 38 30 43	135 38 30 44	135 38 35 43	135 38 35 44	135 38 71 43
135 38 71 44	135 38 72 43	135 38 72 44	135 38 73 43	135 38 73 44	135 38 146	135 39 30 43
135 39 30 44	135 39 35 43	135 39 35 44	135 39 71 43	135 39 71 44	135 39 72 43	135 39 72 44
135 39 73 43	135 39 73 44	135 39 146	135 156 43	135 156 44		

Tabulka A.2.1: Možnosti, jak zašifrovat slovo *allen* „císařskou“ šifrou

Znaky otevřeného textu	Šifrové znaky
a	20, 25, 68, 69, 70
l	38, 39
e	30, 35, 71, 72, 73
n	43, 44
al	135
le	156
en	146

Tabulka A.2.2: Odpovídající část šifrovacího klíče „císařské“ šifry.

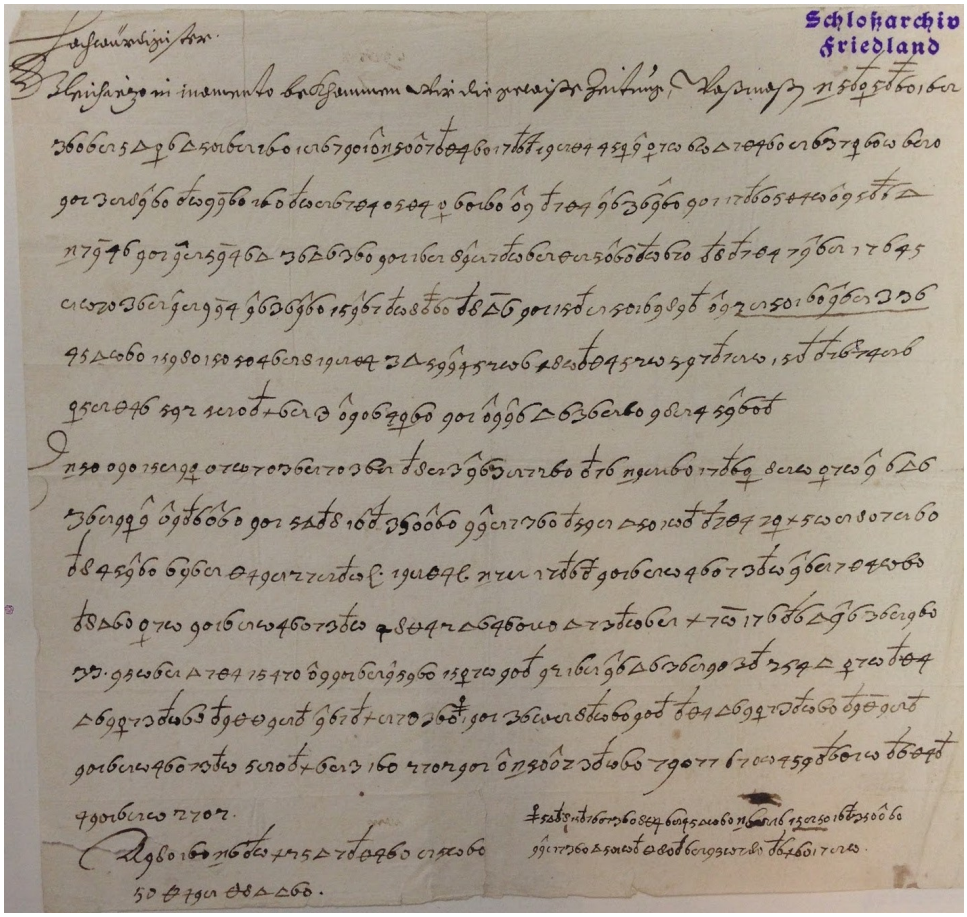
30 43 43 36 45	30 43 43 36 85	30 43 43 66 45	30 43 43 66 85	30 43 83 36 45	30 43 83 36 85	30 43 83 66 45
30 43 83 66 85	30 83 43 36 45	30 83 43 36 85	30 83 43 66 45	30 83 43 66 85	30 83 83 36 45	30 83 83 36 85
30 83 83 66 45	30 83 83 66 85	60 43 43 36 45	60 43 43 36 85	60 43 43 66 45	60 43 43 66 85	60 43 83 36 45
60 43 83 36 85	60 43 83 66 45	60 43 83 66 85	60 83 43 36 45	60 83 43 36 85	60 83 43 66 45	60 83 43 66 85
60 83 83 36 45	60 83 83 36 85	60 83 83 66 45	60 83 83 66 85			

Tabulka A.2.3: Možnosti, jak zašifrovat slovo *allen* „královskou“ šifrou.

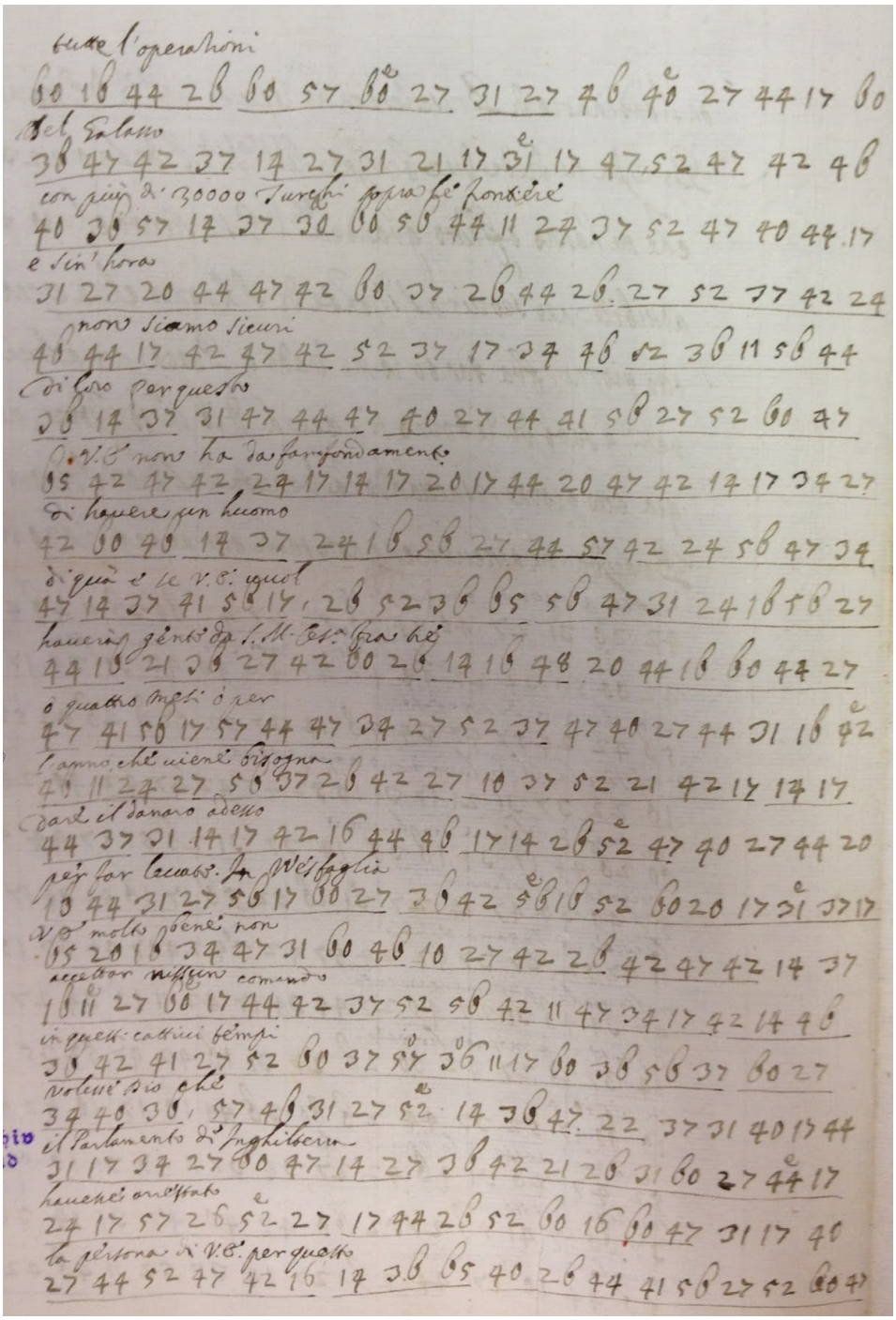
Znaky otevřeného textu	Šifrové znaky
a	30, 60
l	43, 83
e	36, 66
n	45, 85

Tabulka A.2.4: Odpovídající část šifrovacího klíče „královské“ šifry.

A.3 Ukázky šifrovaných dopisů



Obrázek A.3.1: Dopis kurfiřta Ferdinanda z 25. června 1635.



Obrázek A.3.2: Část dopisu Waltera Leslieho z 12. července 1644.